PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-247949

(43)Date of publication of application : 14.09.1998

(51)Int.Cl. H04L 12/66
G09C 1/00
H04L 9/32
H04M 3/00
H04M 11/00
H04N 1/00
H04N 1/32
H04N 1/44

(21)Application number : 09-050137

(22)Date of filing : 05.03.1997

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>

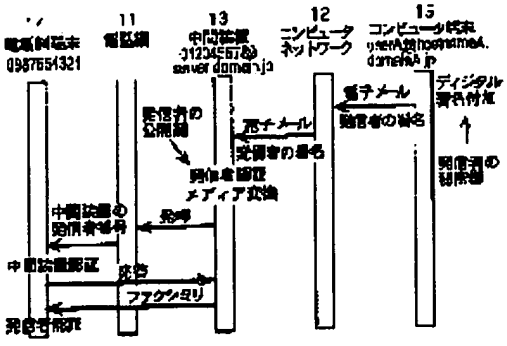
(72)Inventor : YAMADA TOMOHIRO
TAKAHASHI ISAMU
SUZUKI AKIRA

(54) CALLER AUTHENTICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To surely authenticate a caller in the case of communication between a telephone network terminal 14 and a computer terminal 15 via an intermediate device 13.

SOLUTION: A terminal 15 gives a digital signature to a message by using its private key and send the resulting message to an intermediate device 13, and the device 13 authenticates the signature by using a public key and when the signature passes the authentication, the device 13 converts the message into FAX image data and send the data to a terminal 14, the terminal 14 compares the caller number with a caller number of the device 13 stored in advance and receives the FAX data when they are coincident and the terminal 14 authenticates the caller of the terminal 15 from the reproduced image.



* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]A telephone network terminal accommodated in a telephone network and a computer terminal accommodated in a computer network, In a method of attesting an addresser at the time of communicating a message via intermediate equipment (it is only described as intermediate equipment below) with the above-mentioned telephone network, each of the above-mentioned computer network, and an interface, An addresser authentication method attesting a signature of a message which attached to the message a digital signature of an addresser who uses the computer terminal, transmitted to it, and received with the above-mentioned intermediate equipment when sending a message from the above-mentioned computer terminal.
[Claim 2]The addresser authentication method according to claim 1 comparing a sender number which memorized [above-mentioned] the sender number, and attesting intermediate equipment if a sender number of the above-mentioned intermediate equipment is memorized to the above-mentioned telephone network terminal and the above-mentioned telephone network terminal has needed information from the above-mentioned intermediate equipment.
[Claim 3]The addresser authentication method according to claim 2 if the above-mentioned telephone network terminal passes [collation of the above-mentioned sender number], wherein it will attest an addresser by originator information of the above-mentioned computer terminal notified with a message from the above-mentioned intermediate equipment.
[Claim 4]Memorize message ID of a message which received to the above-mentioned intermediate equipment, and the above-mentioned computer terminal gives message ID to the outgoing message, If the above-mentioned digital signature is performed also to this message ID and the above-mentioned intermediate equipment is in agreement as compared with the above-mentioned message ID which memorized message ID in a message from the above-mentioned computer terminal before it, The addresser authentication method according to any

one of claims 1 to 3 processing as an illegal message.

[Claim 5]A telephone network terminal accommodated in a telephone network and a computer terminal accommodated in a computer network, In a method of attesting an addresser at the time of communicating a message via intermediate equipment (it is only described as intermediate equipment below) with the above-mentioned telephone network, each of the above-mentioned computer network, and an interface, An addresser authentication method, wherein the above-mentioned intermediate equipment attaches a digital signature of intermediate equipment to this, and transmits a message which received from the above-mentioned telephone network terminal to the above-mentioned computer terminal and the above-mentioned computer terminal attests a signature of a message which received.

[Claim 6]The addresser authentication method according to claim 5 comparing with a sender number which memorized [above-mentioned] the sender number, and attesting an addresser if a sender number of the above-mentioned telephone network terminal is memorized to the above-mentioned intermediate equipment and the above-mentioned intermediate equipment has the needed information from the above-mentioned telephone network terminal.

[Claim 7]The addresser authentication method according to claim 5 or 6 attesting an addresser by originator information of the above-mentioned telephone network terminal notified with a message from the above-mentioned intermediate equipment if attestation of a signature of the above-mentioned message is passed.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to an addresser's authentication method in the communication which performs message communication mutually between the terminals of a computer network and a telephone network.
[0002]
[Description of the Prior Art]The intermediate equipment (it is only described as intermediate equipment below) 13 which has an interface in each of the public telephone network 11 and the computer network 12 as shown in drawing 12 is formed, The correspondence procedure with which the telephone network terminal 14 accommodated in the telephone network 11 and the computer terminal 15 accommodated in the computer network 12 communicate a message via the intermediate equipment 13 is known.
[0003]Conventionally, with the service which performs message communication mutually, the following two methods are mainly taken as a method of performing addresser attestation for fee collection etc., according to the purpose between the terminals 15 and 14 of such a computer network 12 and the telephone network 11. When registering an e-mail address into the intermediate equipment 13 beforehand and transmitting the E-mail from the computer network 12 side to the facsimile terminal 14 as a telephone network terminal via the intermediate equipment 13, the 1st method, If an E-mail is sent to the intermediate equipment 13 from the dispatch computer terminal 15 as shown in drawing 1, The intermediate equipment 13 performs addresser attestation by comparing with the e-mail address which registered beforehand the mail address of the master station 15 in an E-mail, If the attestation is passed, messages, such as a text (character) in the E-mail received from the computer terminal 15 and a picture, will be changed into a facsimile signal, that is, media conversion is performed, and it transmits to the facsimile terminal 14 of a telephone network to a destination side. If the

facsimile terminal 14 has mail arrival via the intermediate equipment 13, the addressee of the facsimile terminal 14 will check an addresser by said e-mail address attached to the message in the reproduced image of the facsimile terminal 14.

[0004]In [when transmitting a facsimile to the computer terminal 15 from the telephone network terminal 14 side, as it is shown in drawing 2] the intermediate equipment 13, Addresser attestation is not performed [as opposed to / especially / the facsimile received from the terminal 14], but media conversion of the facsimile signal is carried out to the form of an E-mail, and it transmits to the computer terminal 15 of a destination side. The addressee of the computer terminal 15 who received this E-mail checks an addresser by the cover page which the addresser of the terminal 14 added.

[0005]The 2nd method registers ID (user identification information) and the password for attesting an addresser into the intermediate equipment 13 beforehand, When transmitting the E-mail from the computer network 12 side to the facsimile terminal 14 of the telephone network 11 via the intermediate equipment 13, As shown in drawing 3, ID and the password for attesting an addresser with the dispatch computer terminal 15 are attached to an E-mail, Transmit an E-mail to the intermediate equipment 13, and the intermediate equipment 13 performs addresser attestation by comparing with ID in the received E-mail, ID which registered the password beforehand, and a password, If attestation is passed, the message of the E-mail will be changed into a facsimile signal, and it will transmit to the facsimile terminal 14 of a telephone network. The addressee of the facsimile terminal 14 checks an addresser by an addresser's ID added to the reproduced image message of the facsimile terminal 14.

[0006]When transmitting a facsimile to the computer terminal 15 from the telephone network 11 side, As shown in drawing 4, ID and a password for an addresser to attest an addresser to PB sound are entered from the facsimile terminal 14, If the intermediate equipment 13 performs addresser attestation and passes this by comparing with the inputted ID, ID which registered the password beforehand, and a password, it will change into an E-mail the facsimile sent after that, and will transmit to the computer terminal 15. The addressee of the computer terminal 15 checks an addresser by addresser ID added to the message of the E-mail which received.

[0007]

[Problem(s) to be Solved by the Invention]In the 1st conventional method, when an addresser's e-mail address is revealed, he is able for the 3rd person to camouflage an addresser's e-mail address unjustly, and to transmit a message, and it may become disadvantageous to an addresser and an addressee. The 3rd person altered unjustly the message which the addresser transmitted, and there was a problem that it may become disadvantageous to an addresser and an addressee. When transmitting a facsimile to a computer terminal from the telephone network 11, in order not to attest with the intermediate

equipment 13, When the 3rd person transmitted a facsimile unjustly, there was a problem that there was a possibility of becoming an addressee's disadvantage, by transmitting to an addressee the message which there is a possibility of bringing the administrator of the intermediate equipment 13 a disadvantage, and an addresser cannot specify.

[0008]In the 2nd conventional method, he is able for the 3rd person to camouflage an addresser's ID and password unjustly, and to transmit a message like the 1st conventional method, and it may become disadvantageous to an addresser and an addressee. The 3rd person altered unjustly the message which the addresser transmitted, and there was a problem that it may become disadvantageous to an addresser and an addressee. Also when ****(ing) a facsimile from the telephone network 11 to the computer terminal 15, there was a problem that he was able for the 3rd person to do camouflage use of an addresser's ID and password unjustly, and to transmit a message, and it may become disadvantageous to an addresser and an addressee.

[0009]. Solved the problem that this invention became a disadvantage of the administrator of intermediate equipment when the 3rd person turns into an addresser, it clears up, or the 3rd person alters a message and the problem and the 3rd person of an addresser and an addressee of becoming a disadvantage transmit a facsimile unjustly. It aims at proposing an addresser authentication method.

[0010]

[Means for Solving the Problem]It is this invention performing a digital signature, when sending from a computer terminal, and performing addresser attestation using a digital signature added to a message with intermediate equipment, It is performing addresser attestation using a sender number which enables detection of an alteration to prevention and a message of spoofing by the 3rd person, and is notified from a telephone network to dispatch [terminal / telephone network], If prevention of spoofing by the 3rd person is enabled and a telephone network terminal has mail arrival, The addressee enables an addresser's check by performing addresser attestation using a sender number of intermediate equipment notified from the intermediate equipment 13, and originator information in an incoming message, If a computer terminal has mail arrival, the addressee attests intermediate equipment using a digital signature of intermediate equipment added to an incoming message, will be taking out originator information in a message, and will enable an addresser's check.

[0011]

[Function]As opposed to the addresser connected to the computer network in attestation with intermediate equipment, By performing addresser attestation using the digital signature added to the message, if digital signatures differ even if the 3rd person fakes an addresser's e-mail address, it can cancel as an inaccurate message. Since only an addresser can create a digital signature and it differs for every message, it becomes possible to detect, even if it is a case

where a part of message is altered when the 3rd person reproduces a digital signature unjustly and. By giving a digital signature also to the message ID given to a meaning by an electronic mail device, by canceling a message with the same message ID, even if it is a case where the whole message is reproduced unjustly, it becomes detectable. To the addresser connected to the telephone network, it is not from an addresser, but is performing addresser attestation using the sender number notified from a telephone network, and it becomes possible to prevent the 3rd person becoming completely unjustly. The addressee connected to the telephone network also in attestation by an addressee, An addresser's check is attained by performing addresser attestation by acquiring only the sender number of intermediate equipment beforehand using the sender number of the intermediate equipment notified from a telephone network, and the originator information in a message, It is acquiring only the public key of intermediate equipment beforehand, and the addressee connected to the computer network attests intermediate equipment using the digital signature of intermediate equipment, he is taking out the originator information in a message, and an addresser's check of him is attained.

[0012]

[Embodiment of the Invention]

An example of the communications system with which this invention is applied to example 1 drawing 1 A is shown, and identical codes are attached to drawing 12 and a corresponding portion. The telephone network 11 is provided with the sender number reporting means 21. The telephone network terminal 14 is provided with the communication control means 22 which sends and receives a signal with the telephone network 11, In this example, it is a case of a facsimile terminal, and it had the image input output means 23, and has further the sender number extraction means 24 and also the accumulation means 25 which memorizes the sender number of the intermediate equipment 13 from the incoming message in this invention.

[0013]The intermediate equipment 13 is provided with the telephone network 11, and the computer network 12 and the communication control means (interface) 26 and 27 which send and receive communication, respectively, and also in this invention. It has the accumulation means 32 which memorizes the sender number extraction means 28, a means 29 to add a digital signature to an outgoing message, the media conversion means 30, the means 31 that compares a receiving digital signature (verification), a public key still more nearly required for a digital signature and its verification, and a secret key.

[0014]The computer terminal 15 is provided with the communication control means 33 which sends and receives communication with the computer network 12, and the input output means 34 of an E-mail, and also. In this invention, it has the accumulation means 37 which memorizes a means 35 to add a digital signature to an outgoing message, the means 36 which compares a receiving digital signature (verification), a digital signature, a public key required

for that verification, and a secret key.

[0015]Although a digital signature is used in this invention, acquisition of the key needed for this is explained with reference to drawing 2. The intermediate equipment 13 generates the pair of a public key and a secret key, registers a public key into the certificate authority 39, and it memorizes a secret key to the accumulation means 32. The computer terminal 15 acquires the public key of the intermediate equipment 13 from the certificate authority 39, Generate the pair of a public key and a secret key, register the public key into the certificate authority 39, memorize a secret key to the accumulation means 37, and also a digital signature is attached with the secret key of the computer terminal 15 to user's information (ID), such as a self name, This is enciphered by the public key of the intermediate equipment 13, and it transmits to the intermediate equipment 13. The intermediate equipment 13 decrypts those received data with the secret key of the intermediate equipment 13, and acquire the public key of the computer terminal 15 from the certificate authority 39, verify said decryption digital signature by this public key, and if it passes, Carry out accumulation registration of the user's information of the received computer terminal 15 which was decrypted at the accumulation means 32, and the message which shows the registration result is created, On the other hand, it signs with the secret key of the intermediate equipment 13, the registration result message with a signature is enciphered by the public key of the computer terminal 15, and it transmits to the computer terminal 15. The computer terminal 15 decrypts the received encryption data with a secret key, verifies the decrypted signature by the public key of the intermediate equipment 13, and checks the contents of registration.

[0016]This Example 1 is a case where a message is transmitted from the computer terminal 15 to the telephone network terminal 14 via the intermediate equipment 13. In this case, the addresser who uses the electronic mail device (computer terminal) 15 beforehand by for example, the method explained by drawing 2. The subscriber information of the addresser (computer terminal 15) who is information required for attestation is registered into the subscriber information accumulation means 32 in the intermediate equipment 13, The intermediate equipment 13 acquires the public key of the computer terminal 15 required for an addresser's attestation, The addressee who memorizes and uses a facsimile terminal for the subscriber information accumulation means 32 in the telephone network terminal 14 and this example accumulates the sender number of the intermediate equipment 13 required for attestation of the intermediate equipment 13 in the information accumulation means 22 beforehand.

[0017]When transmitting a message from the computer terminal 15, a message is created by the e-mail input output means 34, by the digital signature addition means 35, to said created message, the secret key of the computer terminal 15 is used and an addresser's digital signature is added. The message which added this digital signature is transmitted by the

communication control means 33 to the intermediate equipment 13.

[0018]The intermediate equipment 13 receives this message from the communication control means 27, uses the public key of the computer terminal 15 beforehand accumulated in the accumulation means 32 by the digital signature collation means 31, and compares the digital signature added to the message. As a result of comparing, when a digital signature belongs to an addresser to be sure and it is not altered, it is interpreted as it being a right message, and the contents of the E-mail are changed into a facsimile image by the media conversion means 30. A message is canceled when a digital signature is inaccurate. The message which performed media conversion is transmitted by the communication control means 26 to the telephone network terminal 14. If the call origination to the telephone network terminal 14 occurs from the intermediate equipment 13, the telephone network 11 will notify the sender number of the intermediate equipment 13 to the receiving terminal 14 by the originator information reporting means 21. The receiving terminal 14 extracts a sender number by the sender number extraction means 24, and after checking that it is the receipt from the intermediate equipment 13 with the sender number of the intermediate equipment 13 accumulated in the information accumulation means 25, the communication control means 22 receives a facsimile. Since the addresser's information is added, the reproduced image of the received facsimile can check that an addresser is an addresser registered into the intermediate equipment 13.

[0019]It seems that the E-mail created with the computer terminal 15 is shown in drawing 3. Namely, the addresser address 61 is described first and the format 62 (this example MIME version 1.0) of the following description is shown below, It is described that the partner point (addressee) address 63 is [the theme 64] a test in the Japanese JIS code in this example following this, Next, the inner form 65 shows a boundary by a multi-part/mixing in this example at "... 742959F6218E", After attaching this boundary 66, and it usually being shown for the inner form 67 by this example a text / that a character is a JIS code and also showing that the contents conversion coding 68 is 7-bit numerals in this example, the text 69 which is a message content is described. It is shown behind the next boundary 70 that the inner form 71 is a picture in this example, and that format is gif, it is shown that that contents conversion coding 72 is based on base64 in this example, that coded image data 73 is described below, and the boundary 74 is attached that end.

[0020]The E-mail which signed to this message comes to be shown in drawing 4. That is, the origination address 61, the description format 62, the mail arrival address 63, and the theme 64 are the same as that of drawing 3, and it is the following inner form 65, Become a multi-part and with a signature and a boundary is set to "Next Part Level-1-152633", After it is described that a signature algorithm is pgp-md5 and that it is a message in the next inner form 67 of the boundary 66 and its format rfc822 are described, The description 75 of all the messages in

drawing 3 is made, it is the signature by the pgp method, the signature data 78 follows the inner form 77 following the boundary 76 of the end, and, finally the boundary 79 is attached to it.

[0021]By the media conversion means 30 in the intermediate equipment 13, in this example, the text (character) 69 in an incoming message is changed into the data of a facsimile image as shown in drawing 5, and as the picture message 73 is also shown in drawing 5, it is changed into the data of a facsimile image. In this case, an addresser address and the theme are added to the upper left end of both screens as image data.

[0022]The flow of processing of the example mentioned above is shown in drawing 6. In the computer terminal 15, to the created message, it signs with the secret key of the terminal 15, and sends to the intermediate equipment 13 by making this message with a signature into an E-mail. If a signature is verified and it passes by the public key of the terminal 15, media conversion of the message will be carried out, the telephone network terminal (facsimile terminal) 14 will be called, the terminal 14 checks the sender number of the intermediate equipment 13, and if the intermediate equipment 13 is right, it will answer the intermediate equipment 13 and will receive a facsimile. From the origination address in the reproduced image of the facsimile, it checks being sent from the addresser 15, i.e., a computer terminal. The example of this invention is shown in example 2 drawing 7. This is a case where a message is transmitted to the computer terminal 15 via the intermediate equipment 13 from the telephone network terminal 14.

[0023]The addresser who uses the facsimile terminal 14 as a telephone network terminal registers his sender number with the subscriber information accumulation means 32 in the intermediate equipment 13 beforehand. [required for attestation]The addressee who uses the electronic mail device 15 of a computer terminal acquires the public key of intermediate equipment required for attestation of the intermediate equipment 13 from a certificate authority, and accumulates in the information accumulation means 37. When transmitting a message to the computer terminal 15 from the facsimile terminal 14, a facsimile image as shown in drawing 8 by the facsimile input output means 23 is inputted. The inputted facsimile image is transmitted by the communication control means 22 to the intermediate equipment 13. If call origination occurs from the terminal 14 to the intermediate equipment 13 in that case, the telephone network 11 will notify the sender number of the master station 14 to the intermediate equipment 13 by the originator information reporting means 21. By the sender number extraction means 28, after the intermediate equipment 13 extracts the sender number of a master station, it is compared with the sender number of the terminal 14 accumulated in the subscriber information accumulation means 32. In a right case, by the communication control means 26, the compared result receives a facsimile. When a sender number is not in agreement, it is judged as unjust receipt, and it does not receive. The received facsimile image

is changed into the format of an E-mail as shown in drawing 9 by the media conversion means 30. This E-mail is the origination address 61, the description format 62, the recipient address 63, and the theme 64 (this example FAX) like the case of drawing 3, and that to which the next of the boundary 66 after the inner form 65 was described corresponded with the picture message part in drawing 3 continues.

[0024]The message changed into this electronic mail format adds the digital signature of the intermediate equipment 13 like the case where it is shown in drawing 4, by the digital signature addition means 29. The message which added the digital signature is transmitted to the computer terminal (electronic mail device) 15 by the communication control means 27. After the computer terminal 15 receives a message by the communication control means 33, it uses the public key of the intermediate equipment 13 acquired beforehand for the information accumulation means 37 by the digital signature collation means 36, and compares the digital signature added to the message. If the compared result is right, it can check that an addresser is an addresser registered into the intermediate equipment 13 by the originator information (address) indicated in the From line in the E-mail.

Example 3 -- the difference from Example 1 by the case where this example transmits a message from the computer terminal 15 to the telephone network terminal 14 via the intermediate equipment 13, A digital signature is not given only to the message which the addresser created, A digital signature is given also to the message ID added by the communication control means 33 in the computer terminal 15, it is lost by this that message ID is altered, and it makes it possible to identify a message uniquely by message ID. In order to realize this, it provides, as the ID accumulation means 41 which memorizes the message ID which received in the intermediate equipment 13 shows drawing 1 as a solid line.

[0025]This procedure is shown in drawing 10. The public key of the computer terminal 15 is registered into the intermediate equipment 13 like an example, and the sender number of the intermediate equipment 13 is accumulated in the information accumulation means 25 of the telephone network terminal 14. When transmitting a message from the computer terminal 15, a message is created by the input output means 34, and message ID is added by the communication control means 33 to this message. By the digital signature addition means 35, its digital signature is added to said message, and it transmits to the intermediate equipment 13 by the communication control means 33.

[0026]The user's information beforehand accumulated in the accumulation means 32 is used for the intermediate equipment 13 which received the message by the digital signature collation means 31, and it compares the digital signature added to the message. A message is canceled when a digital signature is inaccurate. As a result of comparing, when a digital signature belongs to an addresser to be sure and it is not altered, it is interpreted as it being a right message, and comparison with all the message ID accumulated in the ID accumulation

means 41 next and the message ID in an incoming message is performed. When message ID differs, the message ID in a message is accumulated in the ID accumulation means 41, and it changes into the data of a facsimile image as showed drawing 5 the contents of the E-mail by the media conversion means 30. When that message ID already exists in the message ID accumulation means 41 as a result of comparison of said message ID, this incoming message judges it as what was reproduced unjustly, and cancels that message. The message which performed media conversion transmits to a facsimile terminal with the telephone network terminal 14 by the communication control means 26. Next processing is the same as that of Example 1.

[0027]It may carry out, as shown in drawing 11 as an acquisition method of a public key. Like the case of drawing 2, the intermediate equipment 13 and the computer terminal 15 generate the pair of a public key and a secret key, respectively, and perform registration for a public key and their information to the certificate authority 39, respectively. I have a certificate of acknowledgement in registration in that case published from the certificate authority 39, and the certificate is accumulated in the accumulation means 32 and 37, respectively. In order to register the user's information into the intermediate equipment 13, the computer terminal 15, If acquire the certificate of the intermediate equipment 13 to intermediate equipment first, and the public key of the certificate authority 39 to the certificate authority 39 is acquired, the certificate of the acquired intermediate equipment is attested using this public key and that attestation is passed, From the certificate, the public key of the intermediate equipment 13 is taken out, the user's information of the computer terminal 15 is enciphered by the public key, it signs by the confidential information of the computer terminal 15 to this, and the encryption user's information with a signature and the certificate of a computer terminal are transmitted to the intermediate equipment 13.

[0028]If the public key of the certificate authority 39 to a certificate authority is received, the certificate of the computer terminal received by this public key is attested in the intermediate equipment 13 and this is passed, If take out the public key of the computer terminal 15 from the certificate, and the public key is accumulated in the accumulation means 32, and the signature of the encryption user's information received by the public key is verified and this is passed, After decrypting the encryption user's information with the secret key of the intermediate equipment 13 and checking whether it is correct by the contents of the user's information, user's information is memorized to the accumulation means 32. The registration result message is enciphered by the public key of the computer terminal 15, and the signature of the intermediate equipment 13 is attached to this, and also the certificate of intermediate equipment is also attached, and the encryption registration result is sent to the computer terminal 15.

[0029]In a similar manner, the computer terminal 15 verifies the signature of a reception

registration result by the public key of intermediate equipment, further, is decrypted with the secret key of the computer terminal 15, and checks the contents of registration. Thus, if the certificate of the computer terminal 15 (intermediate equipment 13) is attached to the message which I get to publish a certificate and transmits from the computer terminal 15 (or intermediate equipment 13) and it transmits to it, The received intermediate equipment 13 (computer terminal 15) can obtain the public key of the computer terminal 15 (intermediate equipment 13) from the received certificate. Therefore, the intermediate equipment 13 does not need to acquire the public key of the computer terminal 15 from the certificate authority 39.

[0030]

[Effect of the Invention]In [according to / as explained above / the invention of claims 1 thru/or 4] registration of the message from the computer terminal 15, It becomes possible to become detectable [the alteration to the prevention and the message of spoofing by the 3rd person] with the intermediate equipment 13, and to detect the duplicate of the message by the 3rd person, and there is an economical effect that fee collection to an addresser is performed correctly.

[0031]According to the invention of claims 5 thru/or 7, in registration of the message from the telephone network terminal 14, prevention of spoofing by the 3rd person is attained with the intermediate equipment 13, and there is an economical effect that fee collection to an addresser is performed correctly. According to the invention of claim 2, in the addresser attestation in a receiving terminal, it is effective in an addresser raising the serviceability that the check in a right paddle is attained, only by acquiring the information on intermediate equipment beforehand.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]The block diagram showing the example of the communications system with which this invention method is applied.
[Drawing 2]The figure showing the procedure of the public key acquisition method used for this invention.
[Drawing 3]The figure showing the example of the message made from the computer terminal 15.
[Drawing 4]The figure showing the example of the E-mail which carried out the digital signature of the message of drawing 3 with the computer terminal 15.
[Drawing 5]The figure showing the example which changed the message of drawing 3 into the facsimile image.
[Drawing 6]The figure showing the sequence of the example of an invention of claim 2.
[Drawing 7]The figure showing the sequence of the example of an invention of claim 5.
[Drawing 8]The figure showing the example of a transmitting facsimile image.
[Drawing 9]The figure showing the example which changed the facsimile image of drawing 8 into the electronic message.
[Drawing 10]The figure showing the sequence of the example of an invention of claim 4.
[Drawing 11]The figure showing the sequence of other methods of public key acquisition.
[Drawing 12]The figure showing the example of the communications system with which this invention method is applied.
[Drawing 13]The figure showing the sequence at the time of sending from the conventional telephone network terminal.
[Drawing 14]The figure showing the sequence at the time of sending from the conventional computer terminal.
[Drawing 15]The figure showing the sequence at the time of sending from the conventional

telephone network terminal.

[Drawing 16]The figure showing the sequence at the time of sending from the conventional computer terminal.

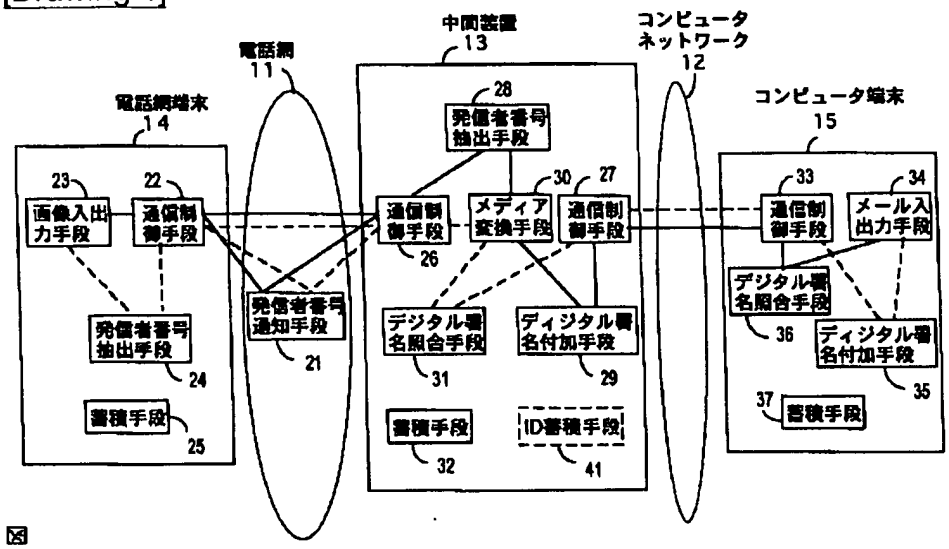
[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

[Drawing 1]



[Drawing 6]

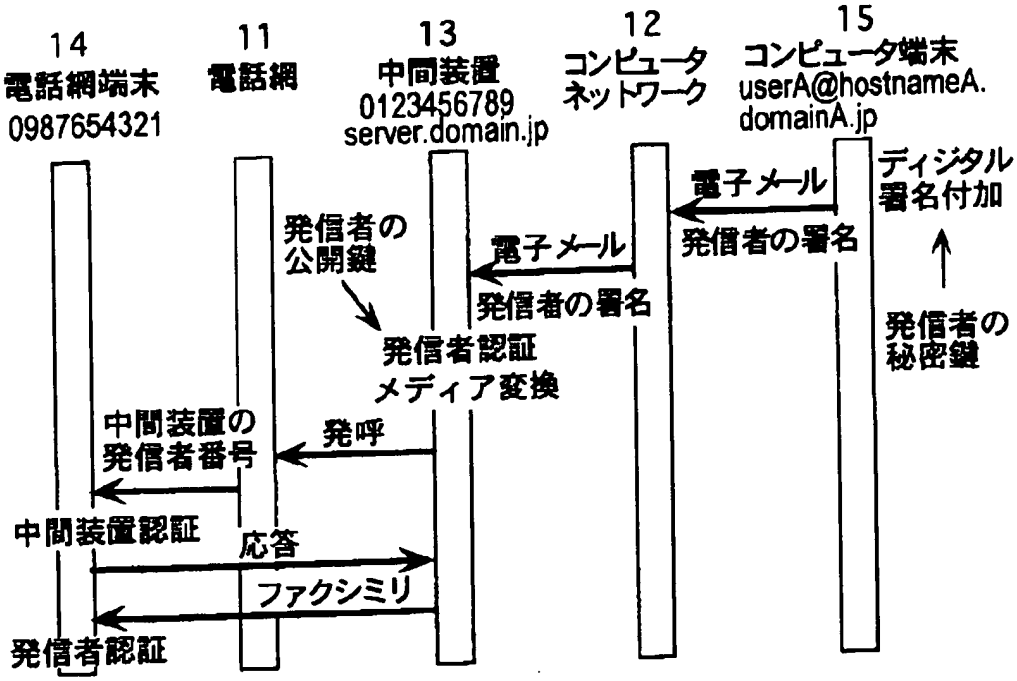

14
電話網端末
0987654321
11
電話網
13
中間装置
0123456789
server.domain.jp
12
コンピュータ
ネットワーク
15
コンピュータ端末
userA@hostnameA.
domainA.jp
電子メール
ディジタル
署名付加
発信者の
公開鍵
電子メール
発信者の署名
発信者の署名
発信者の
秘密鍵
発信者認証
メディア変換
中間装置の
発信者番号
発呼
中間装置認証
応答
ファクシミリ
発信者認証

図 6

[Drawing 2]

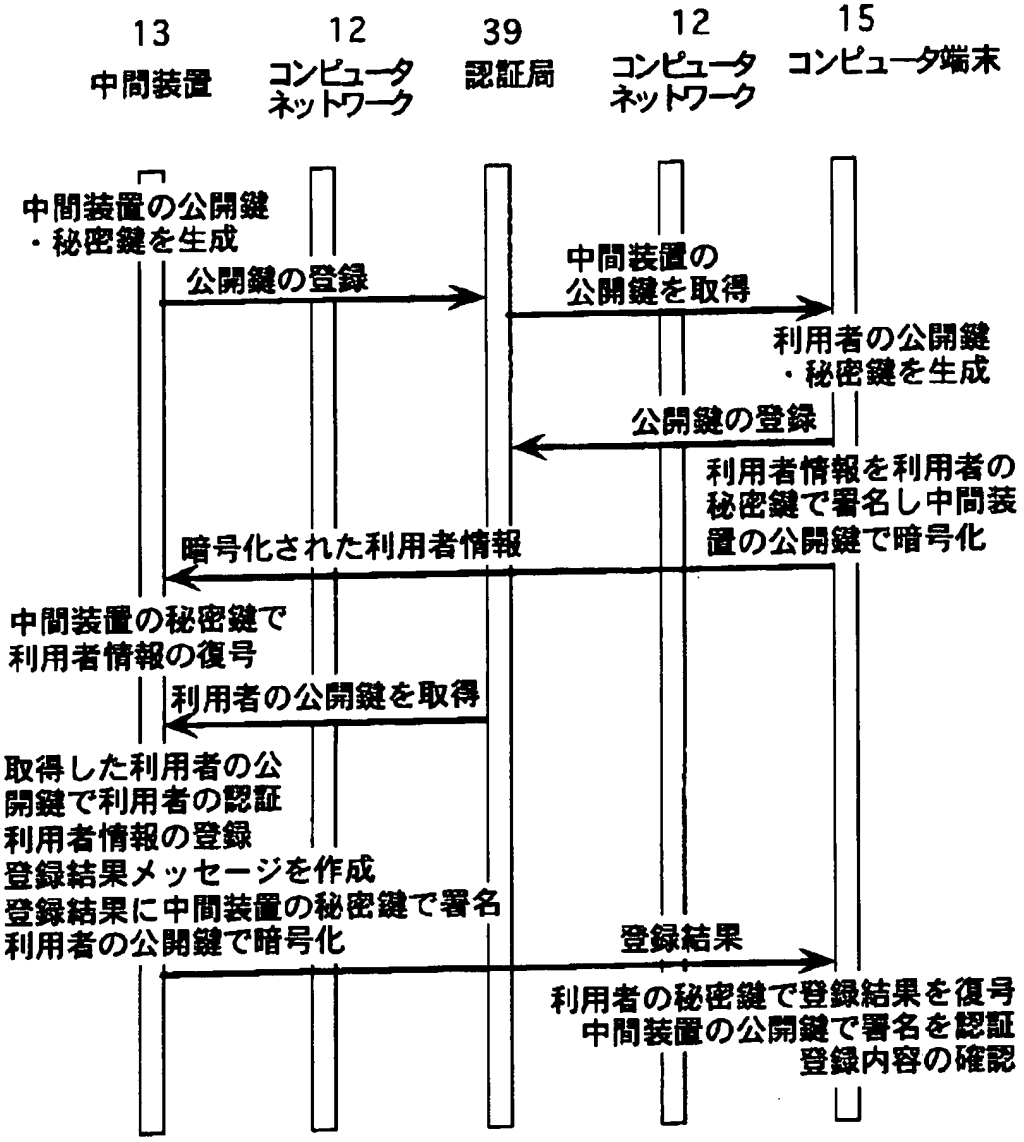


図2

[Drawing 12]

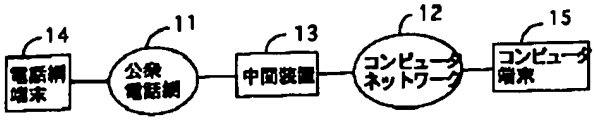


図12

[Drawing 3]

```
From: userA@hostnameA.domainA.jp
MIME-Version: 1.0
To: 0987654321@server.domain.jp
Subject: =?Iso-2022-jp?B?GyRCJUYlOSVlGyhK?=
Content-Type: multipart/mixed; boundary="------742959F6218E"

This is a multi-part message in MIME format.

--------742959F6218E
Content-Type: text/plain; charset=iso-2022-jp
Content-Transfer-Encoding: 7bit

こんにちは。
これはテストです。
--------742959F6218E
Content-Type: image/gif; name="sample.gif"
Content-Transfer-Encoding: base64

R0lGODlhawBaAPcAAP///Hu7Ofb0vfPqsDAwMXFxeG0k8uli
KWlpYWFhXJpZFpaWkA/PjAwM8BYVFQAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
<中略>
mDXSW8oSTgCv5yOtPMZVzKtd9AJFFgWaBTLXa5/7EPiWpURv
R2PhV2dCtDzlZHB7PeFg79CiFg3mxUfEs4vPcnlZxFjQdr+hy7
byAkHXoUhdFKTKDD33JerRZUf9epfnWdykJ4LhryfBU56vlFg/
kMVPPFczHMSaCDKC+MlRBYgbgjRUGQX4D2QbCs92sBSzbpVm
Mi07230gs8lqloQ+ajzJgkBEx+0ABjLJkYwb98jHPvnxj4C8TUA
AADs=
--------742959F6218E----
```

図 3

[Drawing 4]

```
61 From: userA@hostnameA.domainA.jp
62 MIME-Version: 1.0
63 To: 0987654321@server.domain.jp
64 Subject: =?iso-2022-jp?B?GyRCJUYlosvlGyhK?=
65 Content-Type: multipart/signed; boundary="Next_Part_Level_1_152633";
   micalg=pgp-md5;
        protocol="application/pgp-signature"

66 ····Next_Part_Level_1_152633
67 Content-Type: message/rfc822

   From: userA@hostnameA.domainA.jp
   MIME-Version: 1.0
   To: 0987654321@server.domainA.jp
   Subject: =?iso-2022-jp?B?GyRCJUYlosvlGyhK?=
   Content-Type: multipart/mixed; boundary="·····742959F8218E"

   This is a multi-part message in MIME format.

   ·····742959F8218E
   Content-Type: text/plain; charset=iso-2022-jp
   Content-Transfer-Encoding: 7bit

   こんにちは。
75 これはテストです。

   ·····742959F8218E
   Content-Type: image/gif; name="faximage1.gif"
   Content-Transfer-Encoding: base64
   Content-Disposition: inline; filename="faximage1.gif"

   R0lGODlhawBaAPcAAP///Hu7Ofb0vfpqsDAwMXFxeG0k8uliKWlpYWFhXJpZ
   FpaWkA/PjAwMBYVFQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

   <中略>

   IFgfkMVPPFczHMSaCDKC+MRBYgbgRUGQX4D2QbCe92sBSzbpVmMI072
   30gs8IqloQ+ejzJgkBEx+0ABjLJkywb98HPvnj4C8TUAAADs=
   ·····742959F8218E····
76 ····Next_Part_Level_1_1512633
77 Content-Type: application/pgp-signature

   ·····BEGIN PGP SIGNATURE·····
   Version: 2.6.2i

78 iQBVAwUBMvWLWu8FMT+s8kpAQFMCAH/dOXF1AkhNPzsyfffnD3lcowzS9z
   m6KmC2+MvJlhCZlnvZYxEEY4elmq8lgDc9jhwemXnFQ23TEYhGNUHYRTZbg=
   =g0b6
   ·····END PGP SIGNATURE·····
79 ····Next_Part_Level_1_152633-
```

図 4

[Drawing 5]

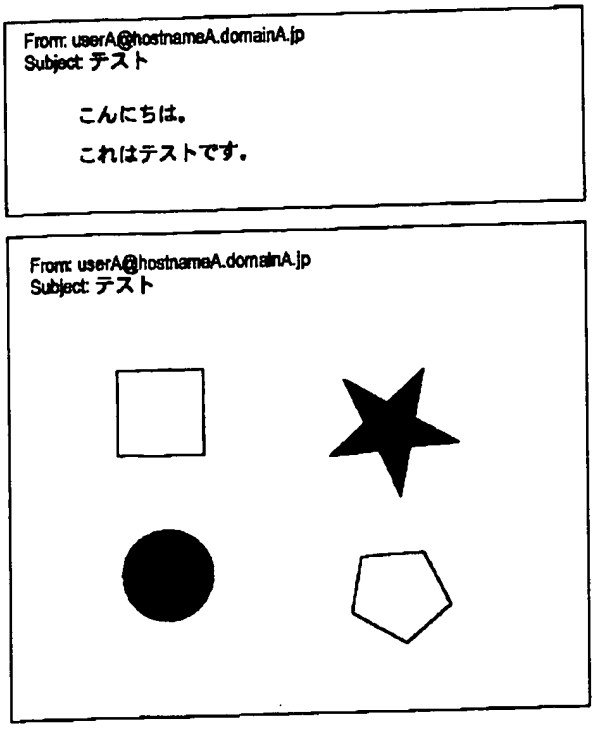


図5

[Drawing 8]

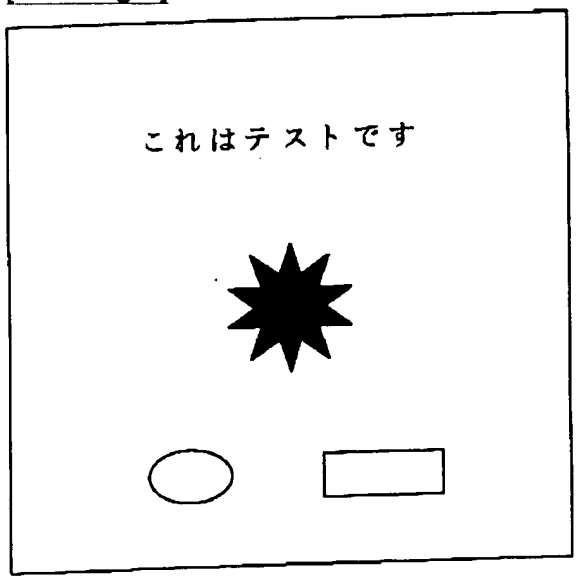


図8

[Drawing 7]

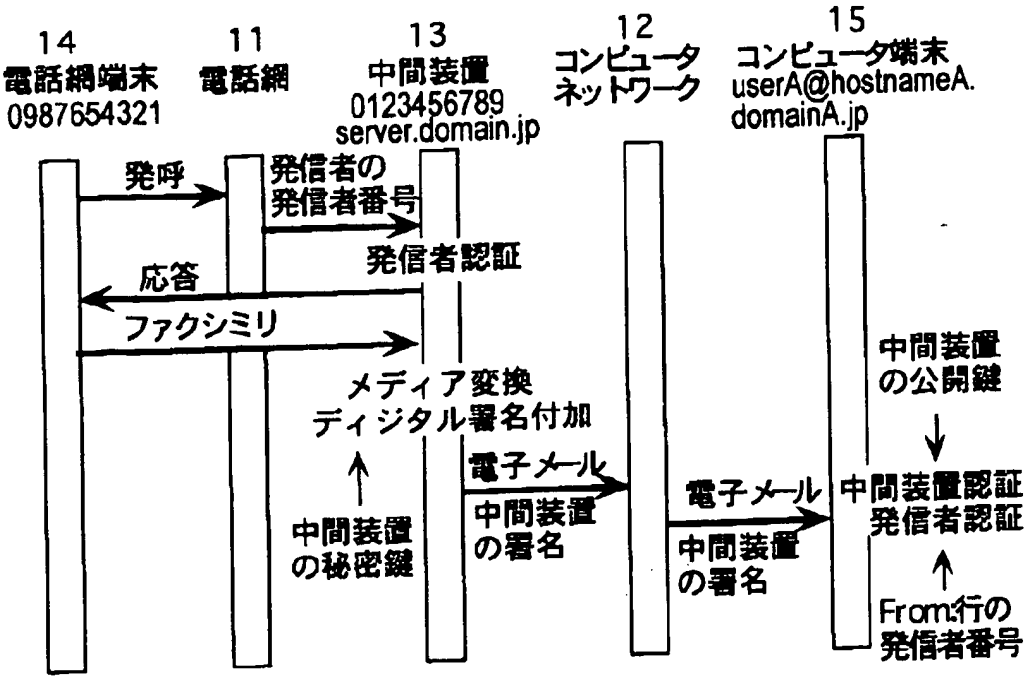


図7

[Drawing 9]

```
61 From: 0987654321@server.domainA.jp
62 MIME-Version: 1.0
63 To: userA@hostnameA.domain.jp
64 Subject: FAX
65 Content-Type: multipart/mixed; boundary="·····742959F6218E"

68 ·····742959F6218E
71 Content-Type: image/gif; name="sample.gif"
72 Content-Transfer-Encoding: base64

73 R01GODdhwAagCIAAAP///wAAACwAAAAAwAagCAAC/4SPqcvtD6
   OctNqLs968+w+G4kiW5omm6sq27gvH8kzX9o3n+s73/g8MCofEovG
   ITCqXzKbzCY1SAqEZVYrNardcF/JL/k7FkuuD7ACnw2lF+bZs82JOf
   lgv3f3fPw9DpEXVZen8fYmh5ih2KHX9wqZKSnFyAAIdxZRlW15Seh
   o6OkW
   <中略>
   9mRRNmXnfYolVGVd9mVhVlfjNWZptmZt9mZdNmd1dmd5tmd99
   meBNqRohXZoibZojfZokTZp1XZpmbZpnfZpoTZqpXZqqbZqrfZqs
   TZrfXZrubZrvfZrwTZsxXZsybZszfZs0TZt1XZt2bZt3fZt4TZu5XZu6b
   Zu7fZu8TZv9XZv+bZvfZvATdwBXdwCbdwDfdwETdxFXdxGbdxEf
   dxITdyJXdyKbdyLfdyMTdzNXdzObdzPfdzQTd0RXd0Sbd0Tfd0UTd
   1VXdlg6AAAAA7

74 ·····742959F6218E····
```

図9

[Drawing 13]

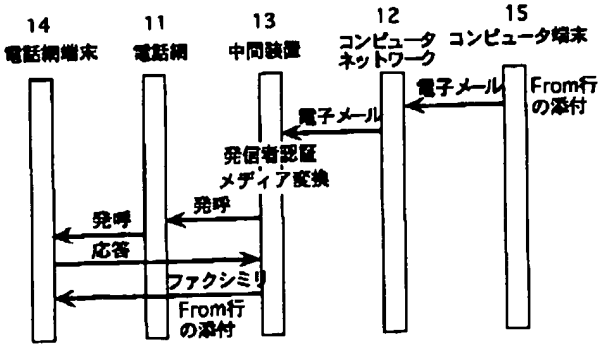


図13

[Drawing 14]

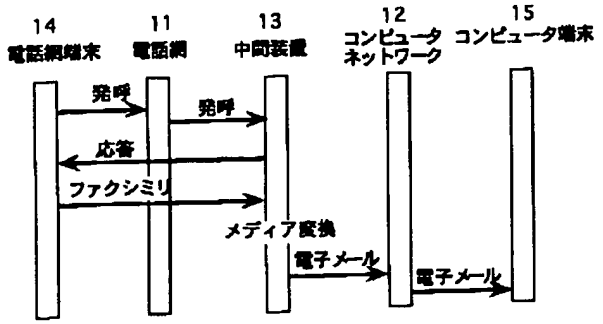


図14

[Drawing 10]

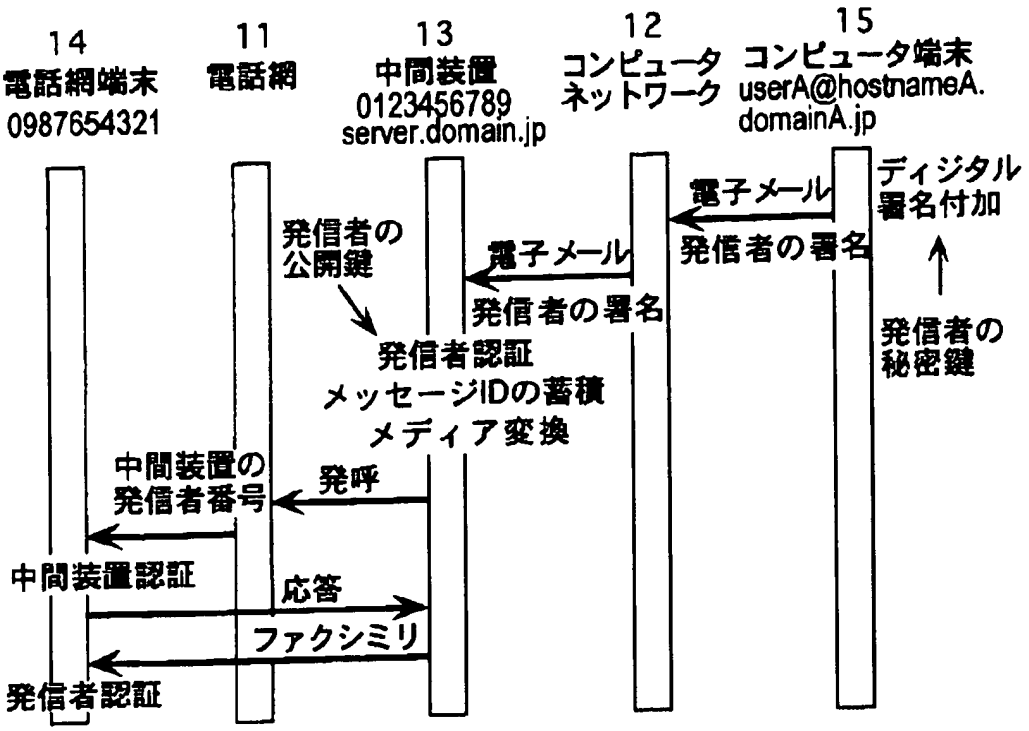


図１０

[Drawing 15]

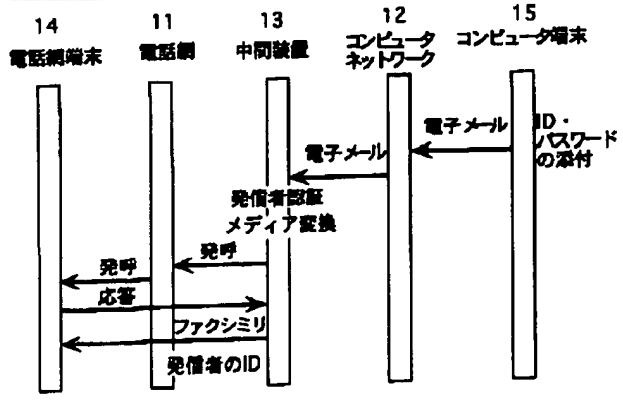


図15

[Drawing 16]

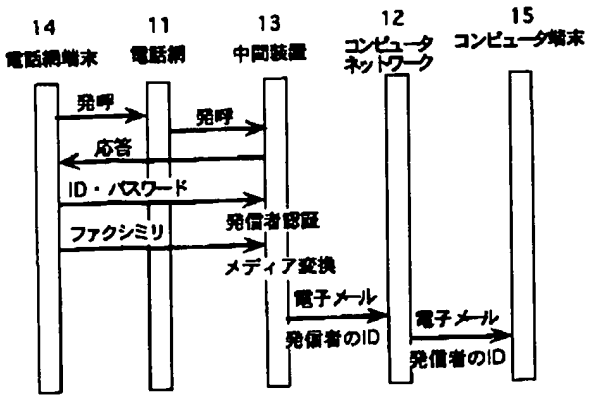


図16

[Drawing 11]

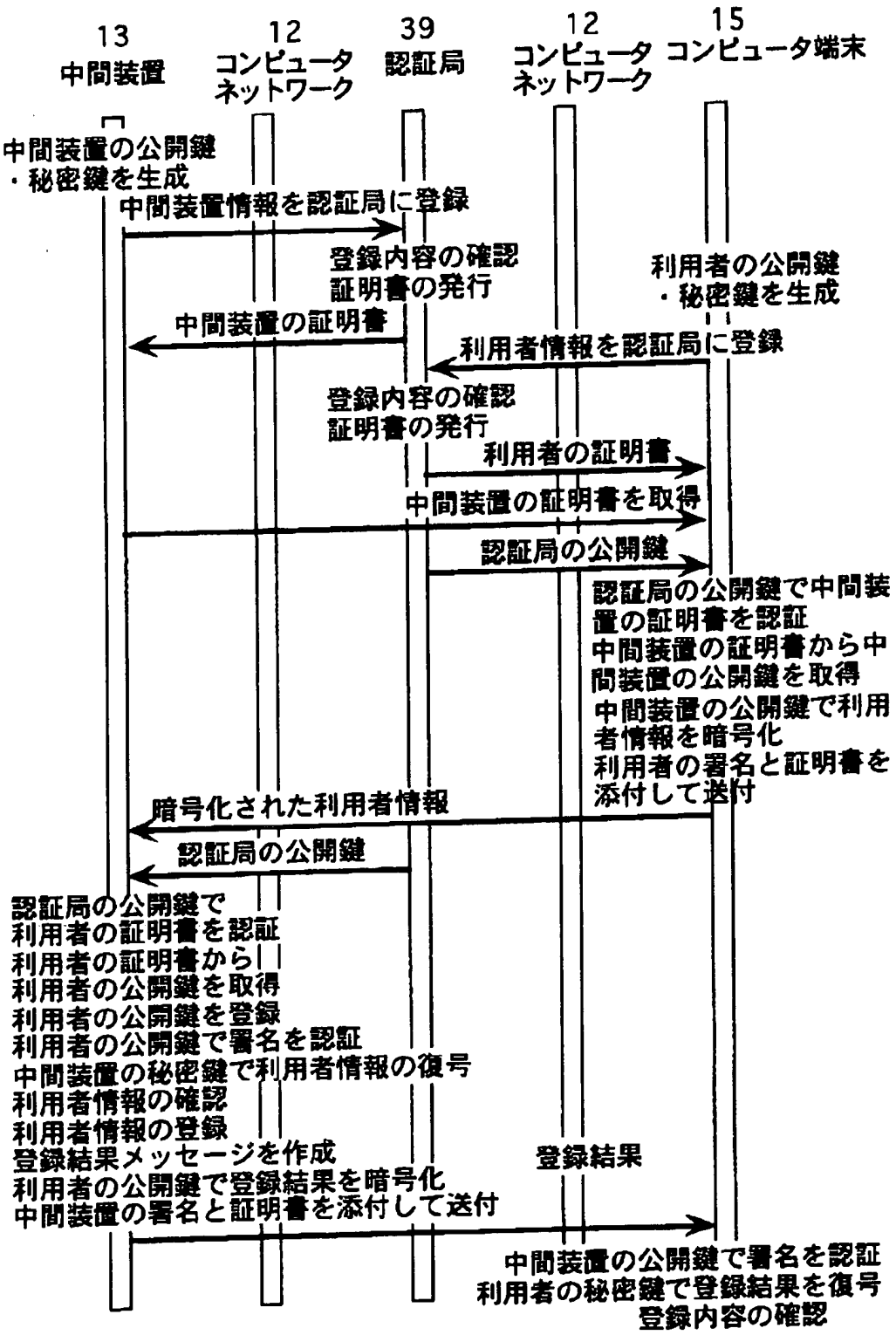


図11

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平10－247949

(43)公開日　平成10年(1998)９月14日

(51)Int.Cl.[6]		識別記号	FI		
Ｈ０４Ｌ	12/66		Ｈ０４Ｌ	11/20	Ｂ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
Ｈ０４Ｌ	9/32		Ｈ０４Ｍ	3/00	Ｂ
Ｈ０４Ｍ	3/00			11/00	３０３
	11/00	３０３	Ｈ０４Ｎ	1/00	１０７Ａ

審査請求　未請求　請求項の数７　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願平9－50137

(22)出願日　平成９年(1997)３月５日

(71)出願人　000004226
日本電信電話株式会社
東京都新宿区西新宿三丁目19番２号

(72)発明者　山田　智広
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　高橋　勇
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(72)発明者　鈴木　晃
東京都新宿区西新宿三丁目19番２号　日本電信電話株式会社内

(74)代理人　弁理士　草野　卓

(54)【発明の名称】　発信者認証方法

(57)【要約】

【課題】　電話網端末１４とコンピュータ端末１５とが中間装置１３を介して通信する際に発信者認証を確実に行う。

【解決手段】　端末１５はメッセージにその秘密鍵によるディジタル署名を付けて中間装置１３へ送信し、装置１３は端末１５の公開鍵で署名を検証し合格すると、メッセージをＦＡＸ画像データに変換して端末１４へ送り、端末１４は発信者番号を予め記憶した装置１３の発信者番号と比較し、一致すればＦＡＸを受信し、その再生画像から端末１５の発信者認証を行う。

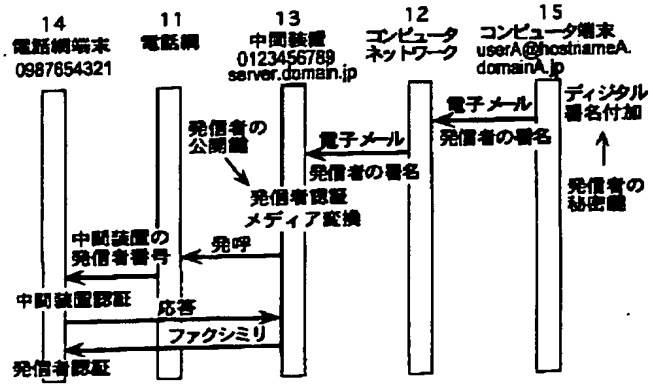


図６

1

【特許請求の範囲】

【請求項１】　電話網に収容された電話網端末と、コンピュータネットワークに収容されたコンピュータ端末とが、上記電話網と上記コンピュータネットワークのそれぞれとインタフェースをもつ中間装置（以下単に中間装置と記す）を介してメッセージを通信する際の発信者を認証する方法において、

上記コンピュータ端末からメッセージを発信する際に、そのメッセージにそのコンピュータ端末を使用する発信者のディジタル署名を付けて送信し、

上記中間装置で受信したメッセージの署名を認証することを特徴とする発信者認証方法。

【請求項２】　上記中間装置の発信者番号を上記電話網端末に記憶しておき、

上記電話網端末は上記中間装置から通信要求があると、その発信者番号を上記記憶した発信者番号とを照合して中間装置の認証を行うことを特徴とする請求項１記載の発信者認証方法。

【請求項３】　上記電話網端末は、上記発信者番号の照合が合格すると、上記中間装置からメッセージと共に通知された上記コンピュータ端末の発信者情報により発信者の認証を行うことを特徴とする請求項２記載の発信者認証方法。

【請求項４】　上記中間装置に受信したメッセージのメッセージＩＤを記憶し、

上記コンピュータ端末はその送信メッセージにメッセージＩＤを与え、このメッセージＩＤに対しても上記ディジタル署名を行い、

上記中間装置は上記コンピュータ端末からのメッセージ中のメッセージＩＤをそれ以前記憶した上記メッセージＩＤと比較し、一致すると、不正メッセージとして処理することを特徴とする請求項１乃至３の何れかに記載の発信者認証方法。

【請求項５】　電話網に収容された電話網端末と、コンピュータネットワークに収容されたコンピュータ端末とが、上記電話網と上記コンピュータネットワークのそれぞれとインタフェースをもつ中間装置（以下単に中間装置と記す）を介してメッセージを通信する際の発信者を認証する方法において、

上記中間装置は上記電話網端末より受信したメッセージを、これに対し中間装置のディジタル署名を付けて上記コンピュータ端末へ送信し、

上記コンピュータ端末は受信したメッセージの署名を認証することを特徴とする発信者認証方法。

【請求項６】　上記電話網端末の発信者番号を上記中間装置に記憶しておき、

上記中間装置は上記電話網端末からの通信要求があると、その発信者番号を上記記憶した発信者番号と照合して発信者の認証を行うことを特徴とする請求項５記載の発信者認証方法。

2

【請求項７】　上記メッセージの署名の認証に合格すると、上記中間装置からメッセージと共に通知された上記電話網端末の発信者情報により発信者の認証を行うことを特徴とする請求項５又は６記載の発信者認証方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、コンピュータネットワークと電話網の端末間で相互にメッセージ通信を行う通信における発信者の認証方法に関するものである。

【０００２】

【従来の技術】図１２に示すように公衆電話網１１とコンピュータネットワーク１２とのそれぞれにインタフェースをもつ中間装置（以下単に中間装置と記す）１３が設けられ、電話網１１に収容された電話網端末１４とコンピュータネットワーク１２に収容されたコンピュータ端末１５とが中間装置１３を介してメッセージを通信する通信方法が知られている。

【０００３】従来、このようなコンピュータネットワーク１２と電話網１１の端末１５，１４間で相互にメッセージ通信を行うサービスでは、課金等のための発信者認証を行う方法として、目的に応じて主に次の２つの方法が取られている。第１の方法は、予め中間装置１３に電子メールアドレスを登録し、コンピュータネットワーク１２側からの電子メールを中間装置１３を経由して電話網端末としてのファクシミリ端末１４へ送信する場合は、図１に示すように、発信コンピュータ端末１５から中間装置１３に電子メールが送られて来ると、中間装置１３は電子メール内の発信端末１５のメールアドレスを予め登録した電子メールアドレスと照合することにより発信者認証を行い、その認証に合格すればコンピュータ端末１５より受信した電子メール内のテキスト（文字）や画像などのメッセージをファクシミリ信号に変換し、つまりメディア変換を行って着信側へ電話網のファクシミリ端末１４へ送信する。中間装置１３を介してファクシミリ端末１４に着信があると、ファクシミリ端末１４の受信者はファクシミリ端末１４の再生画像中のメッセージに添付されている前記電子メールアドレスにより発信者の確認を行う。

【０００４】また、電話網端末１４側からファクシミリをコンピュータ端末１５に送信する場合は図２に示すように中間装置１３においては、端末１４から受信したファクシミリに対しては特に発信者認証を行なわず、そのファクシミリ信号を電子メールの形式にメディア変換して着信側のコンピュータ端末１５へ送信する。この電子メールを受信したコンピュータ端末１５の受信者は端末１４の発信者が付加したカバーページにより発信者の確認を行う。

【０００５】第２の方法は、予め中間装置１３に発信者を認証するためのＩＤ（利用者識別情報）とパスワード

を登録し、コンピュータネットワーク１２側からの電子メールを中間装置１３を経由して電話網１１のファクシミリ端末１４に送信する場合は、図３に示すように、発信コンピュータ端末１５で発信者を認証するためのＩＤとパスワードを電子メールに添付して、中間装置１３に対して電子メールを送信し、中間装置１３は受信した電子メール内のＩＤとパスワードを予め登録したＩＤとパスワードと照合することにより発信者認証を行い、認証に合格すればその電子メールのメッセージをファクシミリ信号に変換して電話網のファクシミリ端末１４に送信する。ファクシミリ端末１４の受信者はファクシミリ端末１４の再生画像メッセージに付加されている発信者のＩＤにより発信者の確認を行う。

【０００６】また、電話網１１側からファクシミリをコンピュータ端末１５へ送信する場合は、図４に示すように、発信者がＰＢ音で発信者を認証するためのＩＤとパスワードをファクシミリ端末１４より入力し、中間装置１３はその入力されたＩＤとパスワードを予め登録したＩＤとパスワードと照合することにより発信者認証を行い、これに合格するとその後送られて来たファクシミリを電子メールに変換してコンピュータ端末１５へ送信する。コンピュータ端末１５の受信者は受信した電子メールのメッセージに付加されている発信者ＩＤにより発信者の確認を行う。

【０００７】

【発明が解決しようとする課題】従来の第１の方法では、発信者の電子メールアドレスが漏洩した場合、第３者が不正に発信者の電子メールアドレスを偽装してメッセージの送信を行うことが可能であり、発信者および受信者に不利益になる場合がある。また、発信者が送信したメッセージを第３者が不正に改ざんし、発信者および受信者に不利益になる場合があるという問題点があった。更に、電話網１１からファクシミリをコンピュータ端末へ送信する際には中間装置１３で認証を行わないため、第３者が不正にファクシミリを送信することにより、中間装置１３の管理者に不利益をもたらすおそれがあり、また、発信者が特定できないメッセージが受信者に送信されることにより、受信者の不利益になるおそれがあるという問題点があった。

【０００８】従来の第２の方法では、従来の第１の方法と同様に、第３者が不正に発信者のＩＤとパスワードを偽装しメッセージの送信を行うことが可能であり、発信者および受信者に不利益になる場合がある。また、発信者が送信したメッセージを第３者が不正に改ざんし、発信者および受信者に不利益になる場合があるという問題点があった。更に、電話網１１からファクシミリをコンピュータ端末１５へ追信する際にも、第３者が不正に発信者のＩＤとパスワードを偽装使用してメッセージの送信を行うことが可能であり、発信者および受信者に不利益になる場合があるという問題点があった。

【０００９】この発明は、第３者が発信者になりすます、あるいは第３者がメッセージを改ざんすることにより発信者および受信者の不利益になるという問題点および第３者が不正にファクシミリを送信することにより中間装置の管理者の不利益になるという問題点を解決した、発信者認証方法を提案することを目的とする。

【００１０】

【課題を解決するための手段】この発明は、コンピュータ端末より発信する場合はディジタル署名を行い、中間装置でメッセージに付加されたディジタル署名を使用して発信者認証を行うことで、第３者によるなりすましの防止およびメッセージに対する改ざんの検出を可能とし、電話網端末よりの発信に対しては電話網より通知される発信者番号を使用して発信者認証を行うことで、第３者によるなりすましの防止を可能とし、電話網端末に着信があると、その受信者は中間装置１３より通知される中間装置の発信者番号および受信メッセージ中の発信者情報を使用して発信者認証を行うことにより発信者の確認を可能とし、コンピュータ端末に着信があるとその受信者は受信メッセージに付加された中間装置のディジタル署名を使用して中間装置の認証を行い、メッセージ内の発信者情報を取り出すことで、発信者の確認を可能とする。

【００１１】

【作用】中間装置での認証において、コンピュータネットワークに接続されている発信者に対しては、メッセージに付加されたディジタル署名を使用して発信者認証を行うことで、第３者が発信者の電子メールアドレスを偽ったとしても、ディジタル署名が異なれば、不正なメッセージとして破棄することができる。また、ディジタル署名は発信者のみが作成できかつメッセージ毎に異なる為、第３者が不正にディジタル署名を複製した場合およびメッセージの一部が改ざんされた場合であっても検出することが可能になる。また、電子メール装置により一意に付与されるメッセージＩＤに対してもディジタル署名を施すことにより、同一のメッセージＩＤを持つメッセージを破棄することで、メッセージ全体を不正に複製した場合であっても検出が可能となる。電話網に接続されている発信者に対しては、発信者からではなく、電話網より通知される発信者番号を使用して発信者認証を行うことで、第３者が不正に成りすますことを防ぐことが可能になる。受信者での認証においても、電話網に接続されている受信者は、予め中間装置の発信者番号のみを取得しておくことで、電話網より通知される中間装置の発信者番号およびメッセージ中の発信者情報を使用して発信者認証を行うことにより発信者の確認が可能となり、コンピュータネットワークに接続されている受信者は、予め中間装置の公開鍵のみを取得しておくことで、中間装置のディジタル署名を使用して中間装置の認証を行い、メッセージ内の発信者情報を取り出すことで、発

信者の確認が可能となる。

【００１２】

【発明の実施の形態】

実施例１

図１Ａにこの発明が適用される通信システムの一例を示し、図１２と対応する部分に同一符号を付けてある。電話網１１は発信者番号通知手段２１を備えているものである。電話網端末１４は電話網１１との信号の送受を行う通信制御手段２２を備え、またこの例ではファクシミリ端末の場合であり、画像入出力手段２３を備え、この発明では更に、受信メッセージから発信者番号抽出手段２４、更に中間装置１３の発信者番号を記憶する蓄積手段２５を備えている。

【００１３】中間装置１３は電話網１１、コンピュータネットワーク１２とそれぞれ通信の送受を行う通信制御手段（インタフェース）２６，２７を備えている他に、この発明では、発信者番号抽出手段２８、送信メッセージにディジタル署名を付加する手段２９、メディア変換手段３０、受信ディジタル署名を照合（検証）する手段３１、更に、ディジタル署名、とその検証に必要な公開鍵、秘密鍵を記憶する蓄積手段３２を備えている。

【００１４】コンピュータ端末１５はコンピュータネットワーク１２との通信の送受を行う通信制御手段３３、電子メールの入出力手段３４を備えている他に、この発明では送信メッセージにディジタル署名を付加する手段３５、受信ディジタル署名を照合（検証）する手段３６、ディジタル署名、その検証に必要な公開鍵、秘密鍵を記憶する蓄積手段３７を備えている。

【００１５】この発明ではディジタル署名を利用するが、これに必要とする鍵の取得について、図２を参照して説明する。中間装置１３は公開鍵と秘密鍵の対を生成して、公開鍵を、認証局３９に登録すると共に秘密鍵を蓄積手段３２に記憶する。コンピュータ端末１５は認証局３９から中間装置１３の公開鍵を取得し、また公開鍵と秘密鍵の対を生成し、その公開鍵を認証局３９に登録すると共に秘密鍵を蓄積手段３７に記憶し、更に自己の名前などの利用者情報（ＩＤ）に対し、コンピュータ端末１５の秘密鍵でディジタル署名を添付して、これを中間装置１３の公開鍵で暗号化して中間装置１３へ送信する。中間装置１３はその受信データを中間装置１３の秘密鍵で復号化し、また、認証局３９からコンピュータ端末１５の公開鍵を取得し、この公開鍵で前記復号化ディジタル署名を検証し、合格すれば、その受信した復号化したコンピュータ端末１５の利用者情報を蓄積手段３２に蓄積登録し、その登録結果を示すメッセージを作成して、これに対し中間装置１３の秘密鍵で署名し、その署名付登録結果メッセージをコンピュータ端末１５の公開鍵で暗号化してコンピュータ端末１５へ送信する。コンピュータ端末１５は受信した暗号化データを秘密鍵で復号化し、その復号化された署名を中間装置１３の公開鍵で検証し、その登録内容を確認する。

【００１６】この実施例１はコンピュータ端末１５から、中間装置１３を経由して、電話網端末１４に対してメッセージを送信する場合である。この場合電子メール装置（コンピュータ端末）１５を使用する発信者は予め、例えば図２で説明した方法により、認証に必要な情報である発信者（コンピュータ端末１５）の加入者情報を中間装置１３内の加入者情報蓄積手段３２に登録しておき、中間装置１３は発信者の認証に必要なコンピュータ端末１５の公開鍵を取得し、加入者情報蓄積手段３２に記憶しておく、また、電話網端末１４、この実施例ではファクシミリ端末を使用する受信者は予め、中間装置１３の認証に必要な中間装置１３の発信者番号を情報蓄積手段２２に蓄積しておく。

【００１７】コンピュータ端末１５からメッセージを送信する際に、メール入出力手段３４によりメッセージを作成し、ディジタル署名付加手段３５により、前記作成したメッセージに対して、コンピュータ端末１５の秘密鍵を使用し、発信者のディジタル署名を付加する。このディジタル署名を付加したメッセージは、通信制御手段３３により、中間装置１３に対して送信される。

【００１８】中間装置１３はこのメッセージを通信制御手段２７より受信し、ディジタル署名照合手段３１により、予め蓄積手段３２に蓄積されたコンピュータ端末１５の公開鍵を使用して、メッセージに付加されたディジタル署名の照合を行う。照合を行った結果、ディジタル署名が確かに発信者のものであり且つ、改ざんされていない場合は、正しいメッセージであると解釈し、メディア変換手段３０により、電子メールの内容をファクシミリ画像に変換する。ディジタル署名が不正であった場合はメッセージを破棄する。メディア変換を行ったメッセージは、通信制御手段２６により、電話網端末１４に対して送信される。中間装置１３から電話網端末１４に対する発呼があると、電話網１１は発信者情報通知手段２１により、中間装置１３の発信者番号を受信端末１４に通知する。受信端末１４は発信者番号抽出手段２４により発信者番号を抽出し、情報蓄積手段２５に蓄積されている中間装置１３の発信者番号により、中間装置１３からの着呼であることを確認したのち、通信制御手段２２によりファクシミリの受信を行う。受信したファクシミリの再生画像は発信者の情報が付加されている為、発信者が中間装置１３に登録されている発信者であることが確認できる。

【００１９】なお、コンピュータ端末１５で作成する電子メールは例えば図３に示すようなものである。即ち、まず発信者アドレス６１が記述され、次に以下の記述のフォーマット６２（この例ではＭＩＭＥバージョン１．０）が示され、これに相手先（受信者）アドレス６３が続き、更に主題６４がこの例では日本語ＪＩＳコードでテストであることが記述され、次に内容形式６５がこの

例ではマルチパート／混合で境界を“・・・７４２９５９Ｆ６２１８Ｅ”で示し、この境界６６を付けて、内容形式６７がこの例ではテキスト／通常、文字はＪＩＳ規格コードであることが示され、更に内容変換符号化６８がこの例では７ビット符号であることが示された後にメッセージ内容であるテキスト６９が記述される。次の境界７０の後に内容形式７１がこの例では画像であり、そのフォーマットがｇｉｆであることが示され、その内容変換符号化７２がこの例ではｂａｓｅ６４によることが示され、次にその符号化された画像データ７３が記述され、その終りに境界７４が付けられる。

【００２０】このメッセージに対し署名した電子メールは例えば図４に示すようになる。つまり発信アドレス６１、記述フォーマット６２、着信アドレス６３、主題６４は図３と同一であり、次の内容形式６５で、マルチパート、署名付きとなり、かつ境界が“Ｎｅｘｔ　Ｐａｒｔ　Ｌｅｖｅｌ－１－１５２６３３”となり、署名アルゴリズムがｐｇｐ－ｍｄ５であることが記述され、境界６６の次の内容形式６７でメッセージであることとそのフォーマットｒｆｃ８２２が記述された後に、図３中の全メッセージの記述７５がなされ、その終りの境界７６に続く内容形式７７にｐｇｐ法による署名であり、その署名データ７８が続き、最後に境界７９が付けられている。

【００２１】中間装置１３内のメディア変換手段３０では、この例では受信メッセージ中のテキスト（文字）６９が例えば図５に示すようにファクシミリ画像のデータに変換され、また画像メッセージ７３も図５に示すようにファクシミリ画像のデータに変換される。この場合、両画面の左上端部に発信者アドレスと主題とが画像データとして付け加えられる。

【００２２】上述した実施例の処理の流れを図６に示す。コンピュータ端末１５では作成したメッセージに対し、端末１５の秘密鍵で署名し、この署名付きメッセージを電子メールとして中間装置１３へ送る。中間装置１３は端末１５の公開鍵で署名を検証し、合格すれば、そのメッセージをメディア変換して電話網端末（ファクシミリ端末）１４を呼出し、端末１４は中間装置１３の発信者番号を確認し、正しければ、中間装置１３に応答し、ファクシミリを受信する。そのファクシミリの再生画像中の発信アドレスから、その発信者、つまりコンピュータ端末１５から発信されたものであることを確認する。

実施例２

図７にこの発明の実施例を示す。これは電話網端末１４から中間装置１３を経由して、コンピュータ端末１５にメッセージを送信する場合である。

【００２３】電話網端末としてのファクシミリ端末１４を使用する発信者は予め、認証に必要な自分の発信者番号を中間装置１３内の加入者情報蓄積手段３２に登録を行う。また、コンピュータ端末の電子メール装置１５を使用する受信者は、中間装置１３の認証に必要な中間装置の公開鍵を認証局から取得し、情報蓄積手段３７に蓄積しておく。ファクシミリ端末１４からコンピュータ端末１５へメッセージを送信する際に、ファクシミリ入出力手段２３により例えば図８に示すようなファクシミリ画像を入力する。入力されたファクシミリ画像は、通信制御手段２２により、中間装置１３に対して送信される。その際に端末１４から中間装置１３に対して発呼があると、電話網１１は発信者情報通知手段２１により、発信端末１４の発信者番号を中間装置１３に通知する。中間装置１３は、発信者番号抽出手段２８により、発信端末の発信者番号を抽出した後、加入者情報蓄積手段３２に蓄積されている端末１４の発信者番号と照合する。照合した結果が正しい場合は通信制御手段２６により、ファクシミリの受信を行う。発信者番号が一致しない場合は不正な着呼と判断し、受信を行わない。受信したファクシミリ画像は、メディア変換手段３０により例えば図９に示すような電子メールのフォーマットに変換する。この電子メールは図３の場合と同様に、発信アドレス６１、記述フォーマット６２、受信アドレス６３、主題６４（この例ではＦＡＸ）であり、内容形式６５が記述された後の境界６６の次は図３中の画像メッセージ部分と対応したものが続く。

【００２４】この電子メールフォーマットに変換されたメッセージは、ディジタル署名付加手段２９により、図４に示した場合と同様に中間装置１３のディジタル署名を付加する。ディジタル署名を付加したメッセージは、通信制御手段２７によりコンピュータ端末（電子メール装置）１５に送信される。コンピュータ端末１５は通信制御手段３３により、メッセージを受信した後、ディジタル署名照合手段３６により、情報蓄積手段３７に予め取得した中間装置１３の公開鍵を使用して、メッセージに付加されたディジタル署名の照合を行う。照合した結果が正しければ、その電子メール中のＦｒｏｍ行に記載されている発信者情報（アドレス）により、発信者が中間装置１３に登録されている発信者であることが確認できる。

実施例３

この実施例は、コンピュータ端末１５から中間装置１３を経由して、電話網端末１４に対してメッセージを送信する場合で、実施例１との違いは、発信者が作成したメッセージにのみディジタル署名を施すのではなく、コンピュータ端末１５内の通信制御手段３３により付加されるメッセージＩＤに対してもディジタル署名を施し、これにより、メッセージＩＤが改ざんされることがなくなり、メッセージＩＤにより、一意にメッセージの識別を行うことを可能とする。これを実現するため、中間装置１３内に受信したメッセージＩＤを記憶するＩＤ蓄積手段４１が図１に実線で示すように設ける。

【００２５】この処理手順を図１０に示す。実施例と同様にコンピュータ端末１５の公開鍵を中間装置１３に登録し、また中間装置１３の発信者番号を電話網端末１４の情報蓄積手段２５に蓄積しておく。コンピュータ端末１５からメッセージを送信する際に、入出力手段３４によりメッセージを作成し、このメッセージに対して通信制御手段３３により、メッセージＩＤを付加する。ディジタル署名付加手段３５により、前記メッセージに対して、自分のディジタル署名を付加して通信制御手段３３により、中間装置１３に対して送信する。

【００２６】メッセージを受信した中間装置１３は、ディジタル署名照合手段３１により、予め蓄積手段３２に蓄積された利用者情報を使用して、メッセージに付加されたディジタル署名の照合を行う。ディジタル署名が不正であった場合はメッセージを破棄する。照合を行った結果、ディジタル署名が確かに発信者のものであり且つ、改ざんされていない場合は、正しいメッセージであると解釈し、次にＩＤ蓄積手段４１に蓄積されている全てのメッセージＩＤと受信メッセージ中のメッセージＩＤとの比較を行う。メッセージＩＤが異なる場合は、メッセージ中のメッセージＩＤをＩＤ蓄積手段４１に蓄積し、メディア変換手段３０により、電子メールの内容を図５に示したようなファクシミリ画像のデータに変換する。前記メッセージＩＤの比較の結果、そのメッセージＩＤがすでに、メッセージＩＤ蓄積手段４１に存在する場合は、この受信メッセージは不正に複製されたものと判断し、そのメッセージを破棄する。メディア変換を行ったメッセージは、通信制御手段２６により、電話網端末１４とのファクシミリ端末へ送信する。この後の処理は実施例１と同様である。

【００２７】公開鍵の取得方法としては例えば図１１に示すように行ってもよい。図２の場合と同様に中間装置１３、コンピュータ端末１５はそれぞれ公開鍵と秘密鍵の対を生成し、公開鍵と自分の情報とをそれぞれ認証局３９に登録を行う。その際に登録内の確認証明書を認証局３９から発行してもらい、その証明書を蓄積手段３２，３７にそれぞれ蓄積しておく。コンピュータ端末１５はその利用者情報を中間装置１３に登録するために、まず中間装置１３から中間装置の証明書を取得し、また認証局３９から認証局３９の公開鍵を取得し、この公開鍵を用いて、取得した中間装置の証明書の認証を行い、その認証に合格すれば、その証明書から、中間装置１３の公開鍵を取出し、その公開鍵でコンピュータ端末１５の利用者情報を暗号化し、これに対するコンピュータ端末１５の秘密情報で署名を行い、その署名付き暗号化利用者情報と、コンピュータ端末の証明書を中間装置１３へ送信する。

【００２８】中間装置１３では、認証局３９から認証局の公開鍵を受取り、この公開鍵で受信したコンピュータ端末の証明書を認証し、これに合格すれば、その証明書からコンピュータ端末１５の公開鍵を取出し、その公開鍵を蓄積手段３２に蓄積すると共にその公開鍵で受信した暗号化利用者情報の署名を検証し、これに合格すれば、その暗号化利用者情報を中間装置１３の秘密鍵で復号化し、その利用者情報の内容に間違いがないかを確認した後、利用者情報を蓄積手段３２に記憶する。その登録結果メッセージをコンピュータ端末１５の公開鍵で暗号化し、その暗号化登録結果を、これに対し中間装置１３の署名を付け、更に中間装置の証明書も付けてコンピュータ端末１５へ送る。

【００２９】コンピュータ端末１５は同様にして、受信登録結果の署名を中間装置の公開鍵で検証し、更に、コンピュータ端末１５の秘密鍵で復号化して登録内容を確認する。このように証明書を発行してもらい、コンピュータ端末１５（あるいは中間装置１３）から送信するメッセージにそのコンピュータ端末１５（中間装置１３）の証明書を付けて送信すれば、受信した中間装置１３（コンピュータ端末１５）は受信した証明書からコンピュータ端末１５（中間装置１３）の公開鍵を得ることができる。従って中間装置１３は認証局３９からコンピュータ端末１５の公開鍵を取得する必要はない。

【００３０】

【発明の効果】以上説明したように、請求項１乃至４の発明によれば、コンピュータ端末１５からのメッセージの受け付けにおいて、中間装置１３で第３者によるなりすましの防止およびメッセージに対する改ざんの検出が可能となり、また、第３者によるメッセージの複製を検出することが可能となり、発信者への課金が正しく行われるという経済的効果がある。

【００３１】また、請求項５乃至７の発明によれば、電話網端末１４からのメッセージの受け付けにおいて、中間装置１３で第３者によるなりすましの防止が可能となり、発信者への課金が正しく行われるという経済的効果がある。また、請求項２の発明によれば、受信端末における発信者認証において、予め中間装置の情報を取得しておくだけで、発信者が正しいかいなかの確認が可能になるというサービス性を向上させる効果がある。

【図面の簡単な説明】

【図１】この発明方法が適用される通信システムの例を示すブロック図。

【図２】この発明に用いられる公開鍵取得方法の手順を示す図。

【図３】コンピュータ端末１５で作られたメッセージの例を示す図。

【図４】コンピュータ端末１５で図３のメッセージをディジタル署名した電子メールの例を示す図。

【図５】図３のメッセージをファクシミリ画像に変換した例を示す図。

【図６】請求項２の発明の実施例のシーケンスを示す図。

【図７】請求項５の発明の実施例のシーケンスを示す図。

【図８】送信ファクシミリ画像の例を示す図。

【図９】図８のファクシミリ画像を電子メッセージに変換した例を示す図。

【図１０】請求項４の発明の実施例のシーケンスを示す図。

【図１１】公開鍵取得の他の方法のシーケンスを示す図。

【図１２】この発明方法が適用される通信システムの例

を示す図。

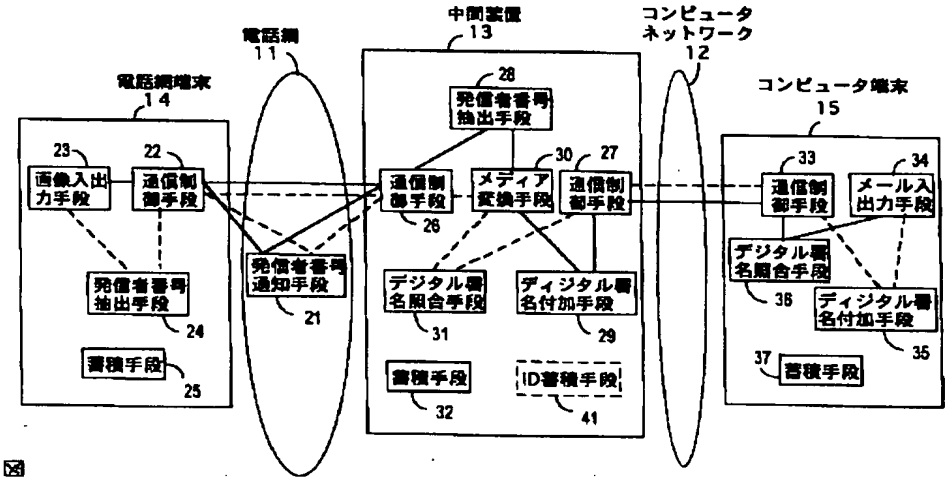
【図１３】従来の電話網端末からの発信した場合のシーケンスを示す図。

【図１４】従来のコンピュータ端末から発信した場合のシーケンスを示す図。

【図１５】従来の電話網端末からの発信した場合のシーケンスを示す図。

【図１６】従来のコンピュータ端末から発信した場合のシーケンスを示す図。

【図１】



図一

【図６】

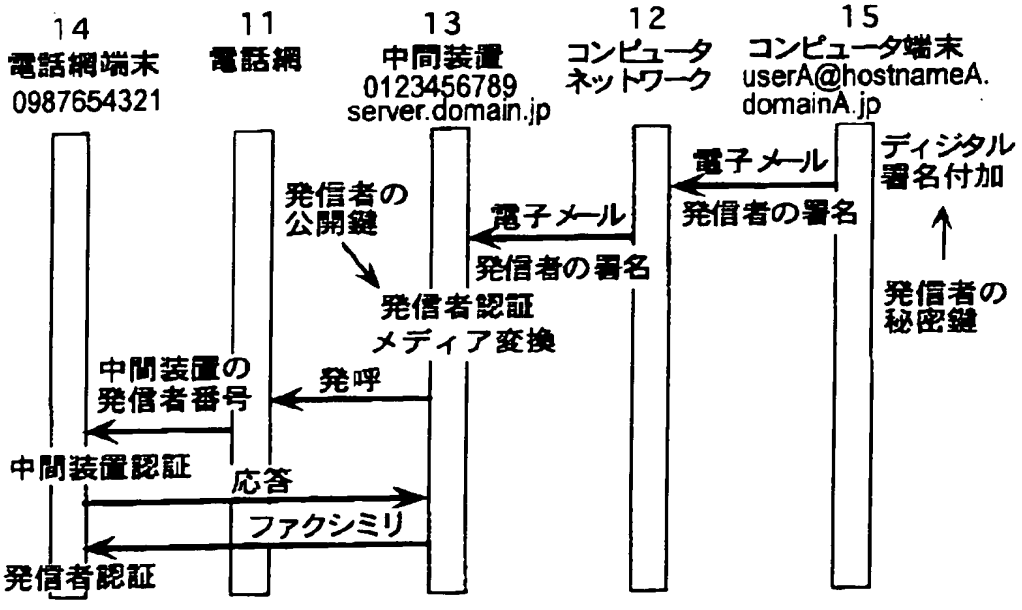


図６

【図２】

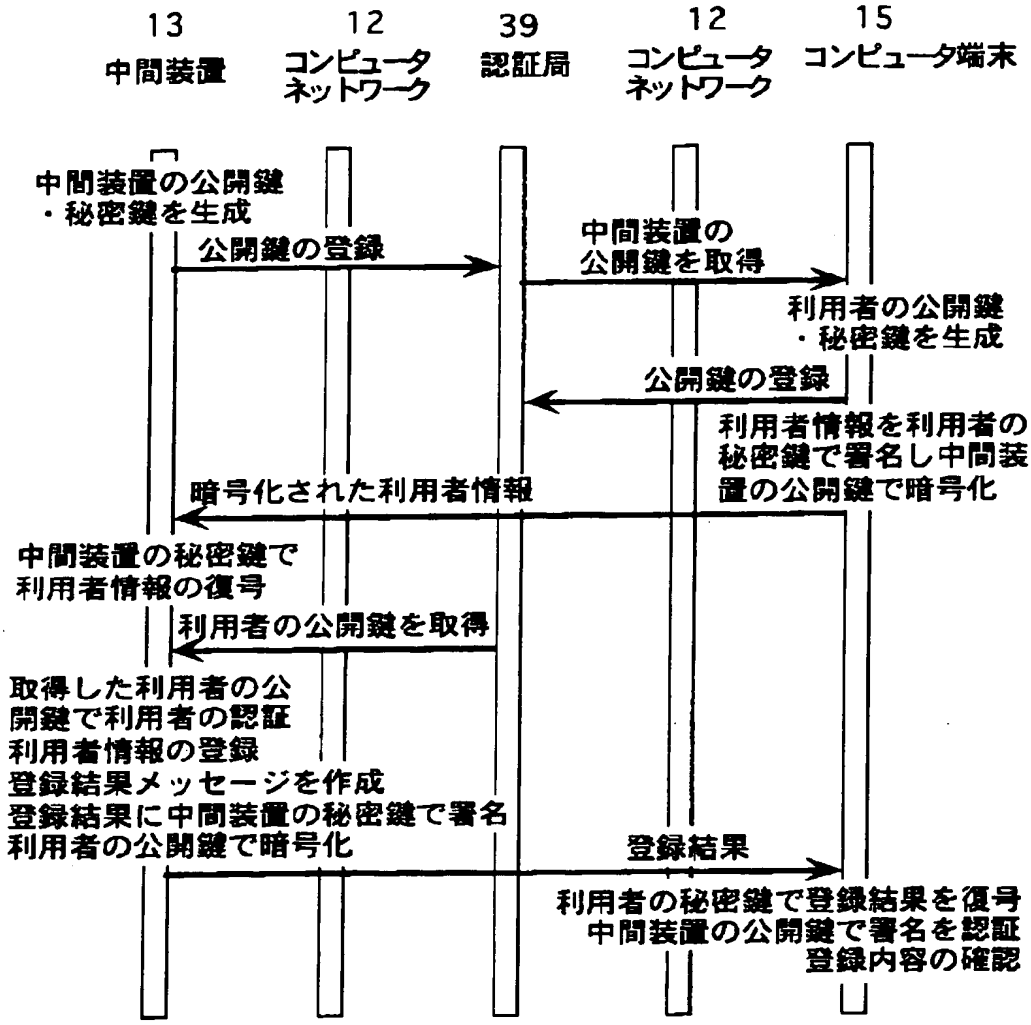

13
中間装置
12
コンピュータネットワーク
39
認証局
12
コンピュータネットワーク
15
コンピュータ端末
中間装置の公開鍵・秘密鍵を生成
公開鍵の登録
中間装置の公開鍵を取得
利用者の公開鍵・秘密鍵を生成
公開鍵の登録
利用者情報を利用者の秘密鍵で署名し中間装置の公開鍵で暗号化
暗号化された利用者情報
中間装置の秘密鍵で利用者情報の復号
利用者の公開鍵を取得
取得した利用者の公開鍵で利用者の認証
利用者情報の登録
登録結果メッセージを作成
登録結果に中間装置の秘密鍵で署名
利用者の公開鍵で暗号化
登録結果
利用者の秘密鍵で登録結果を復号
中間装置の公開鍵で署名を認証
登録内容の確認

図２

【図１２】

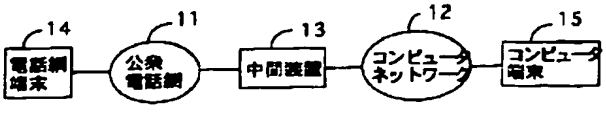

14
電話網端末
11
公衆電話網
13
中間装置
12
コンピュータネットワーク
15
コンピュータ端末

図12

【図３】

```
61 From: userA@hostnameA.domainA.jp
62 MIME-Version: 1.0
63 To: 0987654321@server.domain.jp
64 Subject: =?iso-2022-jp?B?GyRCJUYlOSVlGyhK?=
65 Content-Type: multipart/mixed; boundary="・・・・・・742959F8218E"

   This is a multi-part message in MIME format.

66 ・・・・・・・・742959F8218E
67 Content-Type: text/plain; charset=iso-2022-jp
68 Content-Transfer-Encoding: 7bit

69 こんにちは。
   これはテストです。
70 ・・・・・・・・・・742959F8218E
71 Content-Type: image/gif; name="sample.gif"
72 Content-Transfer-Encoding: base64

   R0lGODlhawBaAPcAAP////Hu7Ofb0vfPqsDAwMXFxeG0k8ull
   KWlpYWFhXJpZFpaWkA/PjAwMBYVFQAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   <中略>
73 mDXSW8oSTgCv5yOtPMZVzKtd9AJFFgWa8TLXa5/7EPiWpURv
   R2PhV2dCtDzlZHB7PeFg79CiFg3mxUfEs4vPcnlZxFjQdr+hy7
   byAkHXoUhdFKTKDD33JerRZUf9epfnWdykJ4Lhryf8U56viFg/
   kMVPPFczHMSaCDKC+MIRBYgbgjRUGQX4D2QbCs92sBSzbpVm
   Mi07230gs8lqloQ+ajzJgkBEx+0ABjLJkYwb98jHPvnxj4C8TUA
   AADs=
74 ・・・・・・・・・・742959F8218E・・・・
```

図３

【図４】

```
61 From: userA@hostnameA.domainA.jp
62 MIME-Version: 1.0
63 To: 0987654321@server.domain.jp
64 Subject: =?iso-2022-jp?B?GyRCJUYlOSVlGyhK?=
65 Content-Type: multipart/signed; boundary="Next_Part_Levl_1_152633";
   micalg=pgpmd5;
        protocol="application/pgp-signature"

66 ・・・・Next_Part_Level_1_152633
67 Content-Type: message/rfc822

   From: userA@hostnameA.domainA.jp
   MIME-Version: 1.0
   To: 0987654321@server.domaine.jp
   Subject: =?iso-2022-jp?B?GyRCJUYlOSVlGyhK?=
   Content-Type: multipart/mixed; boundary="・・・・・・・・742959F8218E"

   This is a multi-part message in MIME format.

   ・・・・・・・・742959F8218E
   Content-Type: text/plain; charset=iso-2022-jp
   Content-Transfer-Encoding: 7bit

   こんにちは。
75 これはテストです。
   ・・・・・・・・742959F8218E
   Content-Type: image/gif; name="faximage.gif"
   Content-Transfer-Encoding: base64
   Content-Disposition: inline; filename="faximage1.gif"

   R0lGODlhawBaAPcAAP////Hu7Ofb0vfpqsDAwMXFxeG0k8uliKWlpYWFhXJpZ
   FpaWkA/PjAwMBYVFQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   <中略>
   iFgAkMVPPFczHMSaCDKC+MIRBYgbgjRUGQX4D2QbCs92sBSzbpVmMi072
   30gs8lqloQ+ajzJgkBEx+0ABjLJkywb98jHPvnxj4C8TUAAADs=
   ・・・・・・・・742959F8218E・・・・
76 ・・・・Next_Part_Level_1_1512633
77 Content-Type: application/pgp-signature

   ・・・・・・・・BEGIN PGP SIGNATURE・・・・・・・・
   Version: 2.6.2i
78 iQBVAwUBMvWLWu8FIMT+s6kpAQFMCAH/dOXF1AkhNPzsyffffnD3icowz59z
   n6KmC2+MvJthCZlnxZYxEEY4emq8lgDc9jhwemXnFQ23TEYHGNUHYRTZbg==
   =g0b6
   ・・・・・・・・END PGP SIGNATURE・・・・・・・・
79 ・・・・Next_Part_Level_1_152633-
```

図４

【図５】

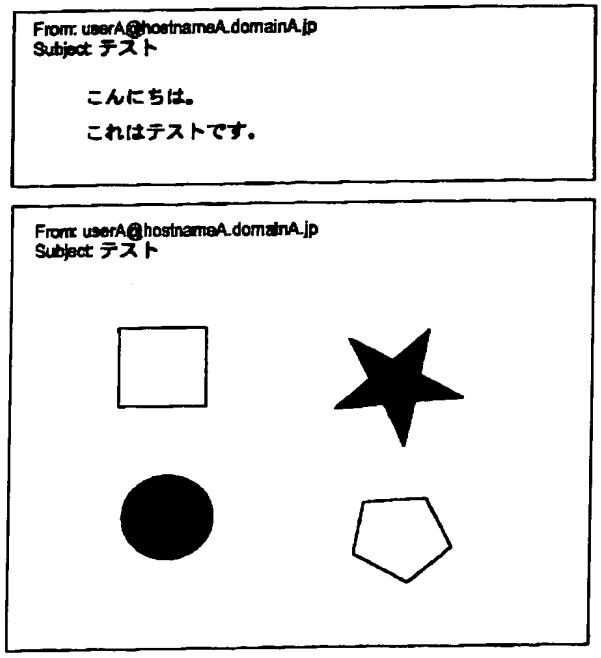


図５

【図８】

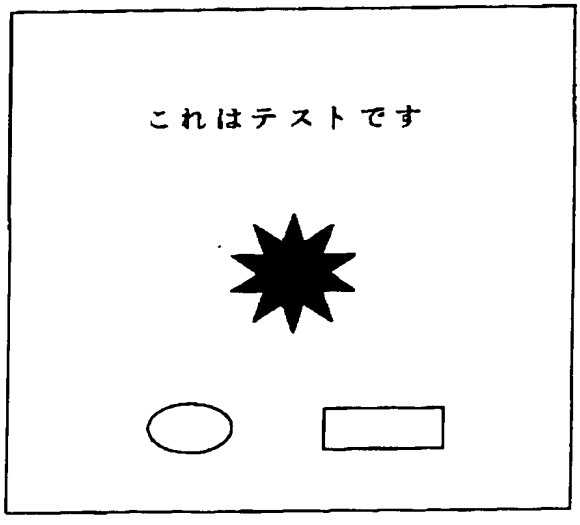


図８

【図７】

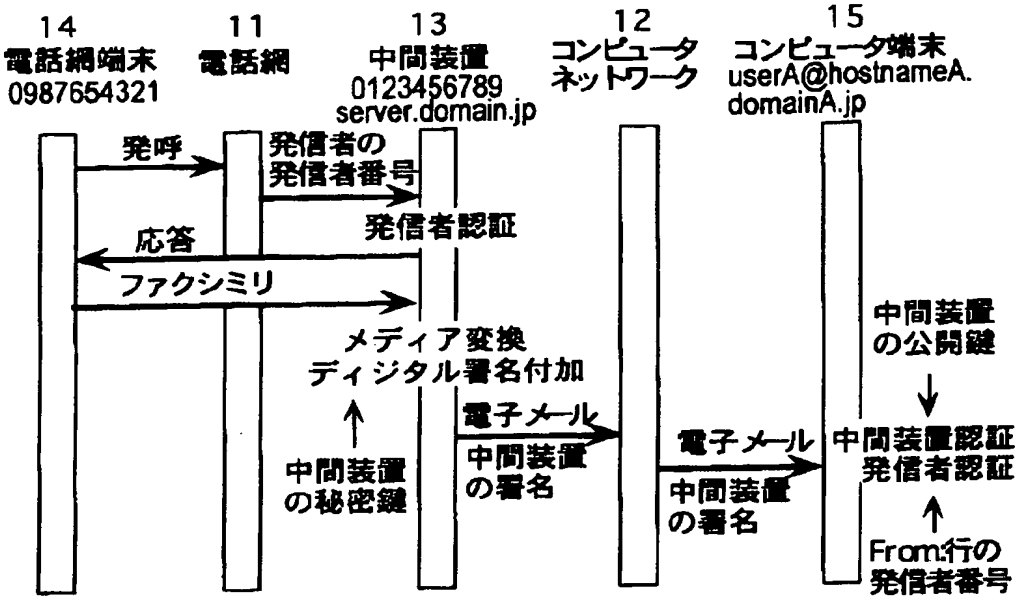


図7

【図９】

```
61 From: 0987654321@server.domainA.jp
62 MIME-Version: 1.0
63 To: userA@hostnameA.domain.jp
64 Subject: FAX
65 Content-Type: multipart/mixed; boundary="·····742959F6218E"

68 ·····742959F6218E
71 Content-Type: image/gif; name="sample.gif"
72 Content-Transfer-Encoding: base64

73 R01GODdhwAagCIAAAP//wAAACwAAAAAwAagCAAC/4SPqcvtD6
   OctNqLs968+w+G4kiW5omm6sq27gvH8kzX9o3n+s73/g8MCofEovG
   ITCqXzKbzCY1SAqEZVYrNardcF/ULlk7FkuuD7ACnw2iF+bZs82JOf
   lgv3f3fPw9DpEXVZen8fYmh5ih2KHX9wqZKSnFyAAIdxZRIW15Seh
   o6OkW
   <中略>
   9mRRNmXnfYoiVGVd8mVhVlfjNWZptmZt9mZdNmd1dmd5tmd99
   meBNqRohXZoibZojfZokTZp1XZpmbZpmfZpoTZqpXZqqbZqrfZqs
   TZrtXZrubZrvfZrwTZsxXZsybZszfZs0TZt1XZt2bZt3fZt4TZu5XZu6b
   Zu7fZu8TZv9XZv+bZvfZvATdwBXdwCbdwDfdwETdxFXdxGbdxEf
   dxITdyJXdyKbdyLfdyMTdzNXdzObdzPfdzQTd0RXd0Sbd0Tfd0UTd
   1VXdlg6AAAAA7

74 ·····742959F6218E····
```

図９

【図１３】

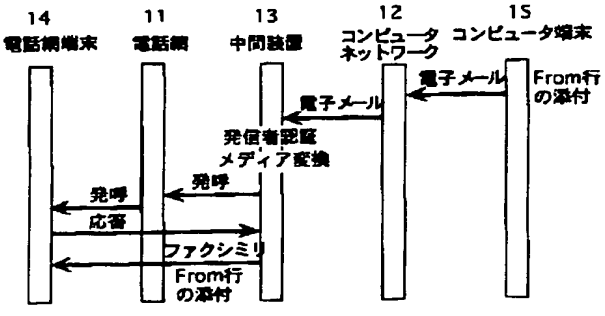


図13

【図１４】

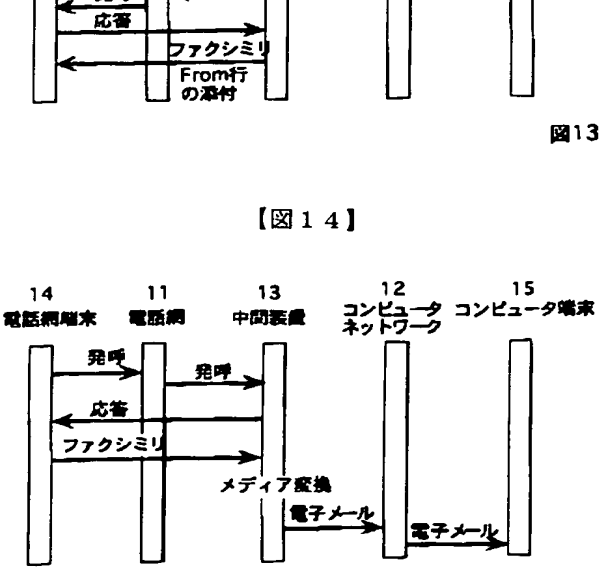


図14

【図１０】

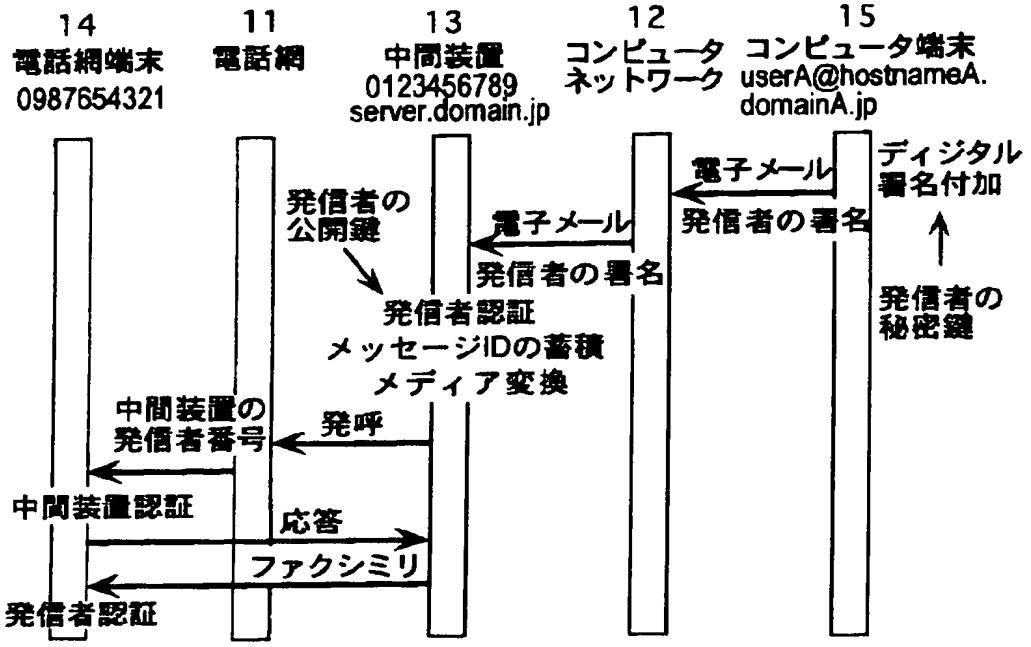


図１０

【図１５】

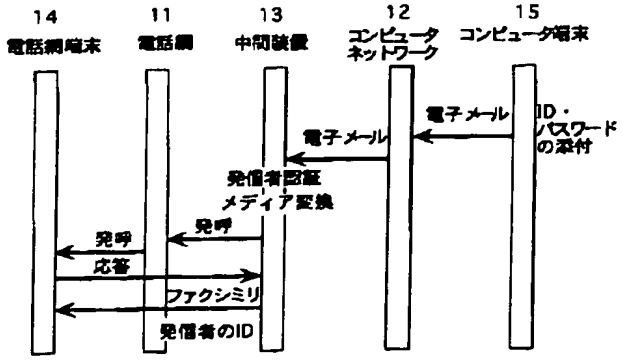


図15

【図１６】

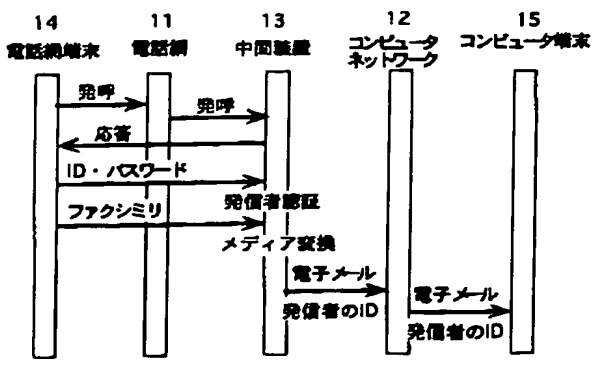


図16

【図１１】

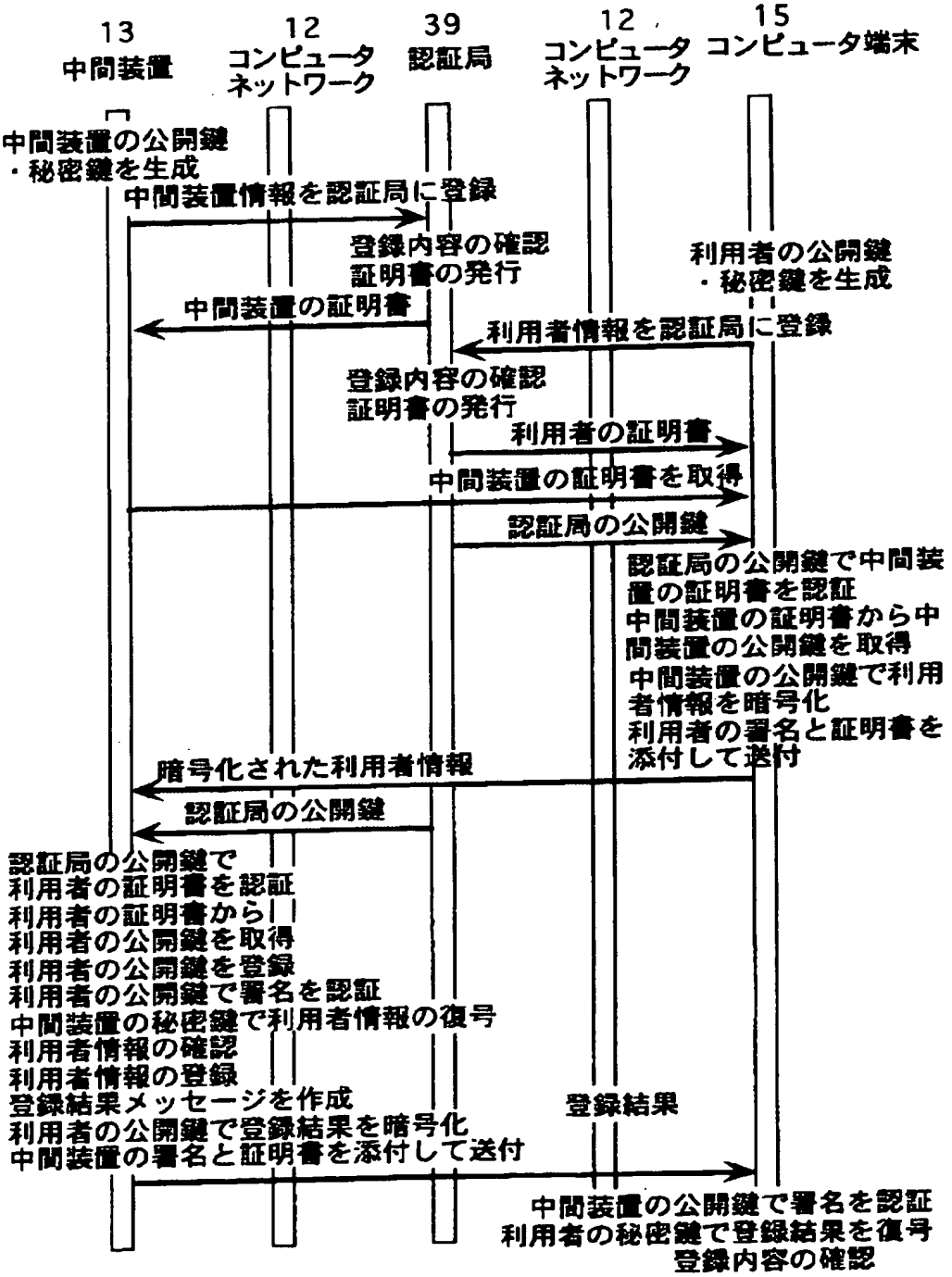

13
中間装置
12
コンピュータネットワーク
39
認証局
12
コンピュータネットワーク
15
コンピュータ端末
中間装置の公開鍵・秘密鍵を生成
中間装置情報を認証局に登録
登録内容の確認
証明書の発行
利用者の公開鍵・秘密鍵を生成
中間装置の証明書
利用者情報を認証局に登録
登録内容の確認
証明書の発行
利用者の証明書
中間装置の証明書を取得
認証局の公開鍵
認証局の公開鍵で中間装置の証明書を認証
中間装置の証明書から中間装置の公開鍵を取得
中間装置の公開鍵で利用者情報を暗号化
利用者の署名と証明書を添付して送付
暗号化された利用者情報
認証局の公開鍵
認証局の公開鍵で
利用者の証明書を認証
利用者の証明書から
利用者の公開鍵を取得
利用者の公開鍵を登録
利用者の公開鍵で署名を認証
中間装置の秘密鍵で利用者情報の復号
利用者情報の確認
利用者情報の登録
登録結果メッセージを作成
利用者の公開鍵で登録結果を暗号化
中間装置の署名と証明書を添付して送付
登録結果
中間装置の公開鍵で署名を認証
利用者の秘密鍵で登録結果を復号
登録内容の確認

図11

フロントページの続き

(51) Int. Cl. 6		識別記号	FI		
H04N	1/00	107	H04N	1/32	Z
	1/32			1/44	
	1/44		H04L	9/00	675B